

CONTENTS

MONITORING PHONE CALLS	4
MORE ON VM/CMS	9
WEATHERTRAK CODES	15
THE HACKER THREAT	16
PRIVATE SECTOR SCAM REVISITED	21
LETTERS	24
A ROLM CATASTROPHE	30
HAPPENINGS	37
2600 MARKETPLACE	41
AT&T/BOC ROUTING CODES	42

2600 Magazine

PO Box 752

Middle Island, NY 11953 U.S.A.

Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Postmaster: Please Send No
Bulk Subscriptions to
2600
© 1986 2600-0001

**DANGER:
MISSING LABEL**

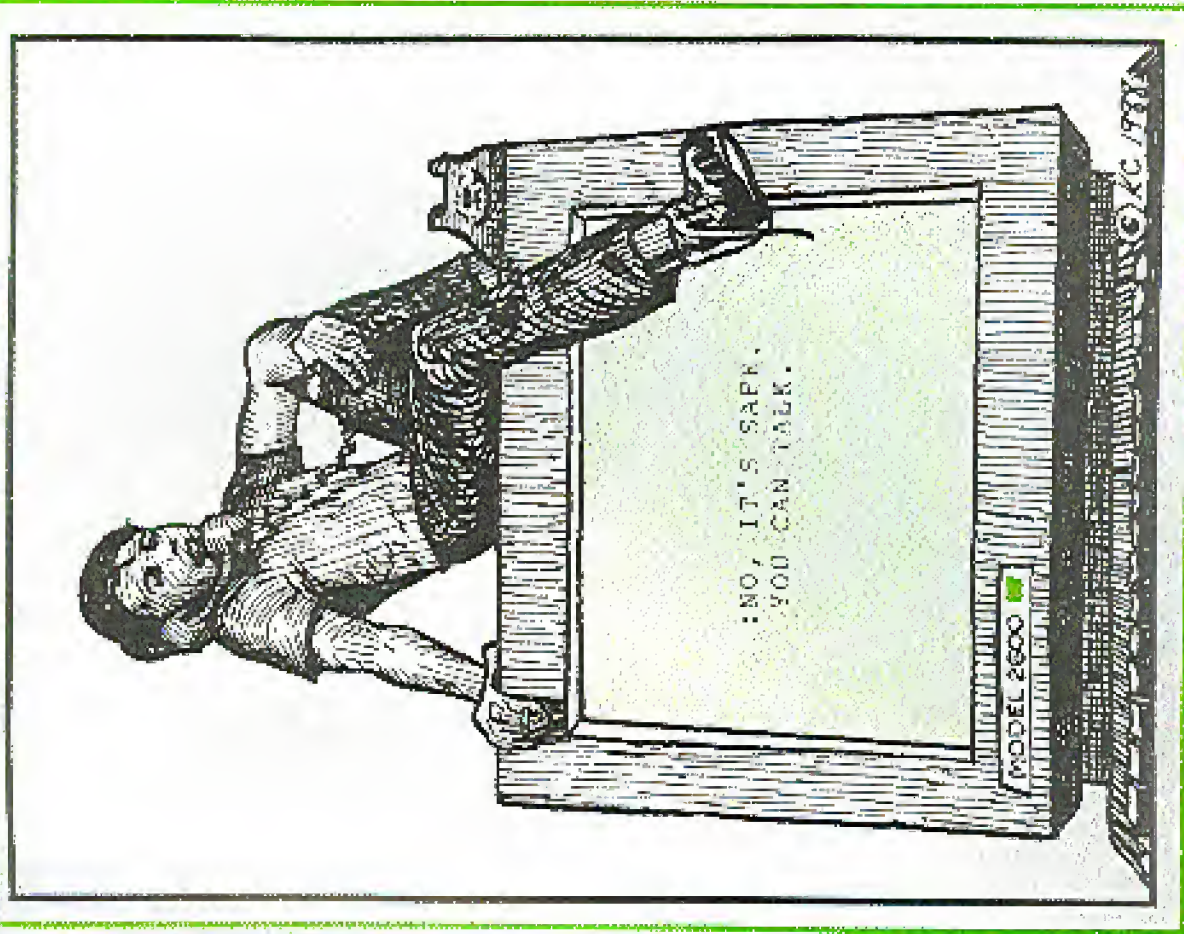
2600

The Hacker Quarterly

Volume 5, Number 1

Spring, 1986

\$4



2600—An independent 1983-84. 5000-51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 843. 844. 845. 846. 847. 848. 849. 850. 851. 852. 853. 854. 855. 856. 857. 858. 859. 860. 861. 862. 863. 864. 865. 866. 867. 868. 869. 870. 871. 872. 873. 874. 875. 876. 877. 878. 879. 880. 881. 882. 883. 884. 885. 886. 887. 888. 889. 890. 891. 892. 893. 894. 895. 896. 897. 898. 899. 900. 901. 902. 903. 904. 905. 906. 907. 908. 909. 910. 911. 912. 913. 914. 915. 916. 917. 918. 919. 920. 921. 922. 923. 924. 925. 926. 927. 928. 929. 930. 931. 932. 933. 934. 935. 936. 937. 938. 939. 940. 941. 942. 943. 944. 945. 946. 947. 948. 949. 950. 951. 952. 953. 954. 955. 956. 957. 958. 959. 960. 961. 962. 963. 964. 965. 966. 967. 968. 969. 970. 971. 972. 973. 974. 975. 976. 977. 978. 979. 980. 981. 982. 983. 984. 985. 986. 987. 988. 989. 990. 991. 992. 993. 994. 995. 996. 997. 998. 999. 1000.

Spring has arrived. And this is the spring issue of 2600. Our new quarterly format has allowed us a bit more time to put together a more cohesive magazine. We hope you're pleased with the result. Never before have so many pages been printed in a hacker publication. There are so many topics to discuss that we refer to our "course". In this issue, you'll find pieces about disastrous telephone systems, the effects of becoming dependent on computers, ways of saving-dropping on telephone

calls in such a way as to be completely undetectable, additions to our previous articles on IBM computer systems, and an interesting look at the world of phone phreaks and computer hackers which contrasts with the way we actually see ourselves. Plus all kinds of numbers, codes, displays, and reproductions that ought to make it off more interesting. If we got so much to say and an increasing number of ways to say it. Our larger but less frequent schedule gives us both the time and the space we need.

(continued on page 8)

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwast

Production
Mike Devouraney

Cover Art
Kent Cappel

Writers: Eric Cawley, John Drake, Mr. French, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOG, David Ruderman, Bernie S., Silent Switchman, Mike Yuhua, and the usual anonymous bunch.

2600 (USPS # 49-801) is published quarterly by 2600 Enterprises, Inc., 7 Murray Lane, Jamaica, NY 11433. Second class postage permit provided at Jamaica, NY 11436.

POSTMASTER: Send address changes to 2600 P.O. Box 52, Middle Island, NY 11953-0052. Copyright © 1988, 2600 Enterprises, Inc.

Yearly subscription: US and Canada \$15 individual, \$50 corporate. Overseas: \$25 individual, \$35 corporate. Back issues available for 1984, 1985, 1986, 1987 at \$25 per year, \$30 per year overseas. **ADDRESS ALL SUBSCRIPTION CORRESPONDENCE:** ED: 2600 Subscription Dept., P.O. Box 792, Middle Island, NY 11953-0072. **FOR LETTERS AND ARTICLES:** SUBMISSIONS, WRITE TO: 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0081.

2600 Office Phone: 516-791-2800
BUS: 516-791-2800
FAX: 516-791-2800
HHS: 516-791-2800
RHS: 516-791-2800
USNET ADDRESS: 3006@ibm.ILL.CAP
ARPANET ADDRESS: phidlaw@129000@mc

monitoring phone calls

This public domain article, written a couple of years back, was obtained from AFRONET. It goes into technical detail on receiving microwave linked telephone conversations using conventional and widely available ham satellite equipment and/or plain satellite TV receiving equipment. Our thanks to the subscriber who sent it in. Regrettably, we don't know who originally wrote the article.

Now that Congress has chosen to attempt to patch a massive hole in the security of communications in the U.S. with a badly drafted law that does not require or even encourage carriers to implement solutions that actually increase real security, I thought I would repost an article I wrote a year ago about a major aspect of the real problem. I hope by so doing to remind everyone that even with draconian law in place it is still very easy to intercept many regular telephone calls and data circuits.

Nothing in the Electronic Communications Privacy Act of 1996 requires or even particularly encourages carriers to increase the security of radio or satellite links. Listeners who get caught can be punished, but nothing has been done to make listening harder.

The kinds of interception I describe are now highly illegal under the new law, but the equipment required is very widely available (and has important legitimate uses that make a ban on sale or possession very unlikely) and the act of interception can be carried out in total secrecy and is nearly impossible to detect from a distance. The Justice department has stated that they do not intend to seriously enforce the radio portions of the law which have been generally recognized to be unenforceable even by the bill's sponsors. So the law, while draconian, really won't leave much of a deterrent effect even as respects casual listeners. And casual listeners are not the real problem.

Yes, it is possible, and not even very difficult. Some years ago it was pointed out that 88 percent of long distance telephone trunks went by ground based microwave. And while the long distance carriers have been working (under some pressure from the NSA and White House) to convert these circuits to optical fibers or at least coaxial cable there are still many routes that use microwave or satellite hops. I don't know an

exact figure but I think it would be reasonable to guess that at least 40-50 percent of long distance trunks include a microwave or satellite hop. And some 75 percent (approximately) of long haul microwave relays use the 3.7-4.2 GHz band which is readily receivable by a TVRO.

Most long haul microwave systems use FM modulation and frequency division multiplexing (FDM) of single sideband suppressed carrier voice channels. Some satellite systems also use this modulation. Unfortunately, FM-FDM-SSB modulation is quite easy to receive with simple and widely available equipment. Recovering the contents of a specific channel is very easy, which opens up the possibility of monitoring random phone calls to a specific group of destinations or monitoring specific private line data or voice circuits (which are assigned to a multiplex slice for long periods of time).

The question of whether a TVRO could be used to monitor phone conversations has been raised on the net. The answer is that with the addition of a stable general coverage single sideband receiver (such as an ICOM R-71 or a Kenwood R-2000 or the receiver section of a modern transceiver) connected to the utilized and unencrypted video output (provided for connecting stereo adapters and desmodulators), a TVRO can be used to listen to FM-FDM multiple level telephone signals from both celestial and ground-based sources.

Further, with a stable down back down converter that converts to the UHF TV band and one of the scanner type receivers designed to cover this band, one can also receive some of the single channel per carrier (SCPC) signals that carry telephone circuits to more remote places (along with network radio feeds, Music, and various broadcast data services such as the AP and UPI news services). (Some signals are filtered and require some form of closed loop A/C to receive them.)

This vulnerability has been well known in security circles for many years, but as the number of TVRO systems has increased to over a million, the problem assumes a somewhat different perspective. In 1976 Mike estimated that it would cost \$50,000+ to intercept microwave telephone calls, and would require a 10 foot dish. In that era a 10 foot dish would

with a TVRO

attract much attention. Today one can buy a TVRO system with a 75" LNA and an 8-12 foot dish for \$1000-\$1500, and almost nobody will give the system a second glance as TVRO's are commonplace. A 75" LNA beats the 10-12 db noise figure receiver that Mike based his calculations on by a very substantial amount. And the current generation of computer controllable general coverage SSB receivers are much cheaper demultiplexing devices than the synthesizer and selective voltmeter (not second necessary in 1976).

"One should not presume that a long distance telephone call is private."

The existence of all these millions of receivers that can pick up both celestial and ground based telephone circuits means that one should not presume that a long distance telephone call is private. And more important (because they are much easier to find in FDM complexes), nobody should assume that a private leased line is secure (unless the long distance carrier has severely limited it via lightweight (than most secure) or oceanic cable (somewhat more secure) for its entire path. (Obviously conventional wireless also have to be considered if there is some reason to believe that some individual or organization has a strong enough reason to be interested in your communications to take the time involved in actually physically tapping your lines.)

Background

Communications satellites carry telephone traffic in several formats. The principle formats are:

Multi Channel systems

1. FDMA-PSK-TDM-PCM

Used on a number of Transponders on 4 and 12 GHz satellites. Heavily used by private business for air lines and other leased line services, sometimes mixed with data. Quite secure if encrypted. Not easily intercepted by private individuals.

2. TDMA-PSK-TDM-PCM

Used on SRS (1/2 GHz) satellites as the principle access technique. Therefore SRS Skyline service and some MCI service (they are now both owned by BBN) is protected this way. Used also on some 4 GHz transponders. Very difficult for private individuals to intercept even if not encrypted. Some circuits are encrypted, same net. TDMA is felt to be the heavy use satellite access technique of the future as it offers very efficient use of transponder power and dynamic allocation of system capacity to those links which are currently active. When combined with encryption it is quite secure.

3. FDMA-FM-FDM-SSB

Standard modulation uses on almost all terrestrial long haul telephone microwave circuits. Used on several 4 GHz downlink transponders and most older multi channel Intelnet links. Widespread FM-FDM signals can be readily received by standard TVRO receivers, and an individual channel can be easily picked out of the multiplex signal with a quality variable general coverage SSB communications receiver. Very easy for private individuals to intercept.

4. CDMA-TDM-PCM, otherwise known as spread spectrum.

CDMA or spread spectrum techniques are widely used on military satellite links because of their security and resistance to jamming. Intercepting and decoding well designed secure spread spectrums grants difficult even for large well equipped intelligence agencies. Doubting sure of the commercial spread spectrum data signals can be accomplished by a private individual with the right equipment, but is moderately difficult.

Single channel systems

5. FDMA-FM otherwise known as SCPC-FM

Single Channel Per Carrier is used to transmit one single bit M telephone channel between two points. A transponder carries many such FM carriers at one time. Frequencies are set after coordination by a central station when the call is set up, and may only be used for the duration of the call. This technique is used for communications with remote probes that rarely need more than a few circuits at once. Can be relatively easily intercepted by a wide band scanner connected to a very stable clock down

(continued on next page)

monitoring phone calls

converter. Easy for private individuals to intercept.

6. FDM-PCM, otherwise known as SCPC-PCM or SPADE.

This technique is the international standard IntelSat method of establishing telephone connections between places that don't have enough traffic to warrant permanently assigned FDM trunks. Each direction of each telephone call is assigned a channel by the central control station. Stations transmit a PSK keyed carrier on that channel for the duration of the call. Each carrier contains one 8 KHz sampled PCM bitstream along with some error correction and synchronization bits. As far as I know, encryption is not used. The signal can be intercepted by a sophisticated individual but intercepting it requires a rather large dish as the effective radiated power per carrier is very much less than domestic SCPC carriers use. A few domestic satcom SCPC users use PCM, probably with some form of encryption. Hard for a private individual to intercept.

7. FM-FDM-FM (Subcarrier on Video Band).

As most TVRO owners discover, many of the video feeds contain additional subcarriers that carry unrelated or tangentially related material. Included among these are one and a half channels that may occasionally carry telephone-like conversations. There are no regular telephone circuits on video subcarriers however. These subcarriers are literally easy to intercept as most TVRO's have tunable audio demodulation.

On FM-FDM-SSB

All it takes to recover FM-FDM-SSB signals is a suitable wideband FM receiver connected to a stable general coverage SSB receiver that tunes the frequency range used for the baseband. TVRO receivers have the correct bandwidth for many such signals and often incorporate provisions for IF filters that can be used to better adapt the receiver to the narrow band signals found on some transponders. And modern general coverage SSB receivers and transceiver receiver sections with synthesized tuning, digital frequency display, and narrow IF filters are well suited to recovering the audio on a particular channel.

Listening to FM-FDM-SSB signals can be accomplished by tuning the TVRO receiver to

either a satellite transponder carrying an FM-FDM-SSB signal (this may involve restricting the 1F bandwidth with a filter as some transponders carry more than one FDM-FM signal), or pointing the antenna at a nearby terrestrial microwave transmitter and tuning the receiver for maximum signal.

Once the FDM-FM signal has been tuned in, the single subband receiver can be used to search the baseband (typically .3 MHz to 6 or 8 MHz) for telephone conversations, 6kHz transmissions, and other private line circuits. Individual channels will appear as USB or LSB signals at precise 4 KHz intervals. In fact, the whole baseband is organized into 12 channel groups, 60 channel supergroups, and 600 channel megagroups according to a standard frequency plan (the ATIS plan as usual) is different from the CCITT one used intentionally.

"Nothing in the Electronic Communications Privacy Act of 1986 requires carriers to increase the security of radio or satellite links."

Most channels have completely suppressed carriers, although certain channels will seem to have a carrier in them (but slightly off frequency, which is something called a pilot tone, used to monitor circuit continuity and control overall gain. Depending on how ancient the telephone trunk equipment is on a particular trunk, it may have a 2500 Hz SF signaling tone in it when it is idle which is dropped when the channel is in use for a call. Trunks which use SF signaling also often use MFMR (multi-frequency key-pulsing—the famous blue box version of tone dialing) to pass telephone numbers on to the destination switch. More modern trunks use OLS (optical control interface signaling) which is a packet network replacement for the earlier and less secure in band signaling that uses separate signalling channels to carry all the signalling for all the trunks in a trunk route.

Obviously, a single signal usually carries only half a telephone conversation so it is necessary to use two receivers and TVRO's to pick up both

with a TVRO

sides of the call clearly. Receiving both sides of a terrestrial circuit requires a suitable location where both directions of transmission can be picked up, which usually means a satellite link with the microwave path. Sometimes both directions of transmission from a single repeater site can be monitored by a very nearby (less than a couple of miles) receiver. Many telephone trunks have low enough echo return loss so that both parties can be heard even when monitoring only one direction of transmission, so it is quite possible to listen to both sides of some conversations with only one receiver. Both sides of a satellite FDM circuit can usually be found on the same bird but are sometimes not, and sometimes not even on FDM sections at all.

In general, particularly on terrestrial signals, all the channels in a 12 channel group originate and terminate at the same place. The groups and supergroups that make up a megagroup however often originate to baseband audio in places. Demodulation to baseband audio is generally done as low lines as possible on a trunk or private line circuit that connects two places; the 12 channels of a group are shifted to various frequencies within the baseband of the different satellite, microwave, or coaxial cable FDM signals that carry it to its destination, but at least with older multiplexing equipment the granularity of routing resolution is usually a group (occasionally half a group), and all 12 of the channels in a group usually end up demodulated to audio at the same place.

Channels within a group are assigned to various purposes. Some may carry telephone trunks, some may carry private line data, some may carry private trunks that belong to large companies, and a certain percentage are reserved for use as spares. It has long been telephone company practice to route the telephone trunks between two switching centers over several different paths to supply redundancy in the event one path fails (and also to make it harder to intercept a particular call between the two switches). This means that any given FDM group may contain trunks from several different trunk groups rather than containing all the trunks from, for example, Chicago to West Bend.

On PSK TDM

The most secure technique in commercial service, and probably the technique that will

perform best on satellite links in the future, is TDM-PCM (time division multiplexed pulse code modulation) either phase shift keying (usually DPSK) or a continuous carrier on a transponder that may have several such carriers on it (TDMA—frequency division multiple access) or keying a single carrier that occupies the whole transponder in bursts precisely timed so as to not overlap other carriers from other stations that it shares a transponder with (TDMA—time division multiple access).

Telephone traffic on TDM-PCM links is sampled 8000 times a second and converted into 8 bit binary values (in a sort of floating point format called A-law or U-law depending that greatly expands the dynamic range from softest to loudest that the channel will handle). (There are other digitizing standards used on satellite phone links but the standard T carrier—D channel bank is widely used.) Some number of these channels (often 24) are combined into a high speed serial bit stream (often 1.554 mb/s) by sending one sample from each channel in serial form as a string of 8 bits followed by a sample from the next channel and so forth. Sometimes this composite bit stream or the bit stream from individual is encrypted with a DES chip. Error correction and framing bits are sometimes special control channel bits are added. This digital bit stream is then serialized (so it has more predictable transition statistics (so it has no DC component) by a laser feedback shift register sequence. The resulting bit stream is used to PSK modulate a carrier which is uplinked to the satellite.

Receiving these FDM-A-PSK-TDM-PCM digital transmissions requires complex RF receivers, a large enough dish to get an acceptable signal to noise ratio (and BESS), and often requires knowledge of DES encryption keys used (unless you are a major intelligence agency and can break DES). While some such transmissions that aren't encrypted could be intercepted by a sophisticated individual, particularly one who had access to the RF receiver and multiplexing hardware used by the subscribers, the required expertise is orders of magnitude greater than that required to intercept FM-FDM-SSB signals and the equipment required is specialized and not widely available. (Decoders for TDM-PCM bit streams could be

(Continued on next page)

(Continued from previous page)

built by a skilled person from available chips relatively easily, but the PSK high speed (if modern technology used would not be easy for even a skilled person to duplicate without substantial resources.) Presumably few if any casual listeners intercept TDM-PCM radio circuits; the only listeners to such transmissions are the intelligence agencies and perhaps industrial spies who can afford to buy the necessary hardware to listen to their competitors' private circuits. And more and more users of such links are encrypting them with DES (which is relatively easy as the information is already in a digital format).

TDMA-PSK-TDM-PCM signals are much more complex than most FDMA-PSK-TDM-PCM signals. This is natural since all traffic is transmitted by having each station on the network transmit a burst at very high speed (tens of mb/s) data in an assigned time slot round robin fashion, included in the burst is all of the traffic that station has with every other station on the network. Every other station monitors all the bursts from stations it is in communication with and picks out the elements that correspond to its incoming traffic. In many such systems, burst lengths and time slots are dynamically assigned by a master ground station computer as calls are

set up and terminated. Each station is capable of receiving and decoding the bursts transmitted by every other station it talks to, so if the channels are not encrypted it could monitor much of or all the traffic going through the transponder.

The burst formats are complex and contain error correction, status and control channels, call setup channels, and so forth. And the bursts are scrambled just as in the ordinary carrier TDMA case. Intercepting and demodulating such a signal would be a major task and is probably something that has only been done (by intelligence agencies) by using specialized versions of the ground station hardware and firmware used by the system. In addition to the complexity of the task of sorting out the digital information and finding the right time slot from the right burst to retrieve the channel of interest, the very high speed fast lock-on RF modules used to demodulate the bursts are themselves non-trivial devices. I suspect that even perverting the firmware in a legitimate ground terminal is complex enough so that no private individual could easily accomplish it without access to a lot of detailed non-published information (such as source of the firmware and precise details of the protocol and burst formats).

(Continued from page 3)

We're happy to announce our affiliation with another computer bulletin board system, our third to date. It's located in Columbus, Nebraska and can be reached 24 hours a day at 402-564-4518. We expect to have more 2600 bulletin boards on line by the summer.

We've also been getting a lot of positive press response in the past couple of months, including a spot on a most incredible television program, Network 7 on England's Channel 4. This program ought to be seen by every reporter in this country who wants to do a story on computer hacking. Instead of looking at the "problem" of hackers and what they could be doing to you in the same way we've seen hundreds of times already,

the producers of this program looked at the positive aspects—the subverters, imagination, and intelligence involved. It wasn't just that they gave hackers a positive image—they used their brains and created a different way of viewing a topic. That's something we can all use a bit more of. Our thanks to John Drake for making this possible.

It's possible the press is finally growing up and realizing that hacking involves so much more than electronic bandwidth. It's a symbol of our times and one of the hopes of the future. If that sounds crazy to you, wander through our pages and it may start to make sense.

by VM guru

As 2600 has published information about various aspects of UNIX and its cousins, my attitude has been more or less hot-hum as I had little interest in these systems. When I saw on the back cover of the November 1987 and December 1987 issues that there was some material on VM/CMS, my interest perked up. That's a system that I know and love, as I have been working as a VM system programmer for many years. The article makes it obvious to me that Lex Lubor, et al has only a superficial knowledge of VM/CMS. I would like to take the opportunity to fill in some of the gaps and give 2600's readers a more complete picture of VM.

Comments on Part 1

A few general points to start:

- There are two types of VM systems. The first is usually fairly small, typically on an IBM 4331, 4341, 4361, or 4381. They are generally unmodified and tend to use the IBM default names for system users and other passwords. Unless you work there, cracking these systems will be difficult because they usually have no data connections to the outside world.
- The other general class of VM system is fairly large, running on a CPU such as a 3081 or 3090. These systems are often modified both to provide function and security. Some of these mods are described below. Many of these mods are passed around at conferences, workshops, or by a conferencing (BBS) system (which will remain nameless).

- The VM system tends itself to modification because most of the source code is distributed with it. For a long time, IBM treated VM as an orphan stepchild and tried to bury it. The users wouldn't let them, and IBM finally recognized it as a going system. VM has now passed through eleven releases, and the twelfth has been announced.
- VM (or CP, the two terms are often used interchangeably) is not an "operating system" in the usual sense of the term. You can't run "jobs" (processes) under it. Rather, you run operating systems under it and each user runs an operating system. Each logged on user gets a "virtual machine" to run his operating system in. Each virtual machine has a CPU, memory (storage), disks, tapes, and unit record (card or printer) devices. Some of these correspond to real devices, and others are virtual. A virtual disk can be represented by a small portion of a real disk. Unit record is usually "spooled" to/from disk. Most systems these days have no real card equipment, and the virtual card equipment allows data to be passed between users as "card images" (80 byte records). All functions that would be buttons, dials, or lights on a real machine are represented by query or set commands to CP in a virtual machine.

- CMS is a single user interactive operating system that is tailored to run very well under VM.
- Other operating systems that are often run under VM are batch systems such as MVS, QJ5/VSE, or VSI. These can run both batch or interactive systems such as TSO, CICS, IDCs, or others. (See the discussion of DIAL below.) A second copy of VM can run under VM, and this is often used to test modifications and new releases. Basically, anything that can be run on the real hardware can be run under VM in a virtual machine.
- VM natively supports three types of terminal. These are 3270 display (DST), video terminals (the many flavors), 2741/15767 (typewriter-like terminals), and ASCII terminals (such as the IBM 3101, TTYs, and ASCII CRTs (such as the VT-100) in line mode. A PC that emulates one of these can also be used. To support ASCII CRTs in full screen, a protocol converter is needed. Both hardware and software versions of protocol converters are available. These make the ASCII CRT look to the VM system as if it were a 3270 terminal. Various escape sequences are used to simulate 3270 functions that the ASCII CRT may not have.

- To cover Lex Lubor's article point by point: (When I refer to commands, I will use the IBM standard names. Some installations have modified these names.)
- While it was late in coming, VM has had online help for some time. It's slow, it's clunky, but it's there. Enter "HELPHELP" to get started.
- While the system is in some what outbalance, that's mainly because of the wealth of functions available. If you found it hard to learn, then either you didn't have the manuals that are needed, or you had a poor teacher (or

modified these names.)

(Continued on next page)

VM/CMS CORRECTIONS

(continued from previous page)

- **bell.** VM/CMS is just too big to pick up on your own without some guidance.
- I won't comment on the acronym list except to say that it only scratches the surface.
- The " " prompt is only seen logging on via an ASCII terminal, and is a "go ahead" signal. Most other terminals supported by VM can have their keyboards locked by VM. It can be turned off, and a common modification is to replace it, sometimes with a "bell" character.
- The "VM/370 ONLINE" prompt (followed by the list of acceptable commands in newer versions of VM) is the only IBM-supplied connection prompt. It is often replaced by the system or company name. The other connection responses Lex mentions are from front end processors or networks, and precede the actual connection to the VM system.
- While some other IBM systems do require it, it is not correct that users (or passwords or even commands) in VM/CMS have to start with a letter. An all numeric userid or password is valid (but not commonly used), and the "national" characters '\$', '@', and '#' can also be used. Certain characters are used as editing characters. A pound sign ('#') is a logical line end. It can be used to separate multiple commands or data lines entered at one time on one terminal line. An at sign ('@') is a character-delete character. One or more at signs will delete the same number of previously entered characters, perhaps saving the retying of a long line. For example, if "aaaaaaaa" is entered, it would be interpreted as "ab". For total foul-ups, the caret sign will tell VM to ignore everything to the left of it so you can start again. For ASCII terminals that don't have a caret sign, the VM system uses the left square bracket instead. And what do you do if you want to enter one of these characters as data? That's where the fourth one comes into play. If any of them is preceded by a double quote, the character pair will be treated as a single data character; i.e. "a" will be treated as a pound sign without being used as an editing character. All of these can be changed to whatever character (not A-Z or 0-9) you wish or they can be turned off. The character-delete is often set to a backspace character if the terminal has that key (most IBM typewriter terminals don't). The "QUERY TERMINAL" command will display the current settings of these characters as well as show other information.
- Some VM security packages use a password up to 24 characters long. (More on them later.)
- Lex is correct that the only currently used IBM login qualifier is "KIDNEY", but others such as terminal type or altering the virtual storage size are common ones. An obsolete qualifier of "MASK" used to be used to tell VM to type a mask (overprinted lines of " ", "H", and "S") so that when you typed your password over the mask, it could not be read. MASK is now the default, and will be ignored if entered. Most larger installations use the password suppression option.
- A common mod is that if an invalid userid is entered, prompt for the password anyway, and then reject the attempt no matter what password is entered.
- Messages warning of exceeding the invalid password threshold are sent to the system operator and/or the system security administrator. It is also recorded in the system's journal (accounting) file.
- The reason that "BONEHEAD" (whose Lex's example is "not valid before login" is that because of the extensibility of VM/CMS, BONEHEAD could very possibly be a valid command, either local to one user, a group of users, or systemwide.
- In a large system, it will be very unlikely to find any passwords that are the same as the userid, or are still at the IBM-supplied defaults. Many security packages force a user to change his password at regular intervals.
- Just because you see a userid, don't make any assumptions about what it does. For example, a large American university has a userid up and running which is the name of the security package they use. It's a dummy, and the security package actually runs under a very innocent userid.
- The DIAL command is used when the operating system running in a virtual machine is a multi-user system such as TSO, CICS, J005, another copy of VM, etc. DIAL establishes a connection between a real terminal, and a virtual port defined for the multi-user system. Security in this case is the responsibility of the multi-user system, except that an available mod requires a password to do a DIAL. Other available mods



Bell of Pennsylvania
A Bell Atlantic Company

To Our Valued Customer:
Here Is Your New Directory

**If Your New Directory
Is Damaged, Call
1-800-555-5000**

**We Will Replace It
Free Of Charge**



Yellow

BELL ATLANTIC CUSTOMERS RECENTLY RECEIVED THIS BURN ON A PLASTIC BAG CONTAINING THEIR NEW YELLOW PAGES. WE'RE GLAD SOMEONE'S FINALLY REALIZED THE DANGERS THAT YELLOW PAGES CAN POSE TO KIDS.

(continued from page 10)

more specific real terminals to connect only to specific ports (or port groups).

- A message to the operator as Lex suggests will bring the security administrator down on you in many systems. In most VM systems, the operator could not give you the password, as he has no access to the directory. In many larger systems, the OPERATOR id (which doesn't have to be called OPERATOR) is disconnected and is running a program called PRQP (Programmed Operator). PRQP will respond to routine messages and route others to "logical operators" such as disk operator, tape operator, or security admin.

- On the monitoring and recording of invalid and privileged commands, this is available as part of standard VM. Because the VM monitor function has high overhead, it is (usually) not done on a regular basis, but is turned on for sample periods or when a problem is suspected. There are mods and packages available which will record all valid and invalid command usage and the resources that the command consumes with minimal overhead.

- The QUERY NAMES command could (on a large system) show several hundred logged on users. An available mod limits it to users in the same group as yours, either by using the account code or a portion of the userid. The order shown has no connection with the order that users logged on. It is simply following an internal channel list of all users, and it stops when it gets back to you. This list has three parts. Above the "VSM—....." line, users are logged in with locally attached (or in some cases, TMINET or its IRLD terminals). The three-digit (four in some larger systems) hex number following the userid is the hex hardware address of the terminal. If your userid is shown in this section, your userid will be the last one in the list. The "VSM—....." line identifies the "VTAM SERVICE MACHINE". This is the link into an IBM SNA (System Network Architecture) network. Users listed below there are connected to VM through a VTAM network which could span many processors and many nodes. The name following the userid is the LU (Logical Unit) name of the terminal, which is used as a network address. These two portions of the list will be absent if the VM system is not connected to an SNA network. The last portion will be missing if the system is

connected to an SNA network, but no users are currently logged on here it.

- On a QUERY USERS response, the number of USERS and NET will be the number of users in the first and last parts respectively of the QUERY NAMES list. The DIAL ED number is the number of users connected to multi-user systems.

- One type of multi-user system you could DIAL to is called a "session manager". This allows you to create several "logical terminals" and log each one onto a different userid (or DIAL to a different system). These logical terminals will show in a QUERY NAMES list as "xxxx" where xxx is a three-digit hex number which can range from 000 to FFF. For logical terminals, the program accepts the data that is to be displayed on the terminal, and simulates entering data on the keyboard. In many systems, creation of a logical device is made a privileged function to reduce the likelihood of a hacker making a "rogue horse". The session manager allows you to switch between your various sessions, with the active one showing on the real terminal. Session managers are usually used with video terminals (CRTs).

"While the system is somewhat cumbersome, that's mainly because of the wealth of functions available."

- A disconnected user (shown on a QUERY NAMES as "OSC") can remain logged on indefinitely. It will only be logged off by the system after 15 minutes (modifiable) if it tries to read from the terminal it doesn't have. OSC users are usually service machines such as security, accounting, utility, database, and other functions. Some large systems have 50 to 100 of them running.

- "Userid NETLOG" is located on your logon, and contains information on files that you SEND to others, and that you RECEIVE from others. It is logged when you receive the file, not when they send it to you. The "USERID" in the name will be your userid, not the userid you sent the file to.

Comments on Part 2

The second part of the article on VM/CMS is just as full of errors and misconceptions as the first. As it part one I will address Lex's article point by point with expansions and advice as appropriate.

- Local commands: This is one of the strong points of VM/CMS. That is, it can be extended with local commands. These can be in any of the three flavors of exec languages (unprivileged, concurrent processor) or any compiled language. To execute it, just have it on any disk that is available to you (private, public) and call it by name. Getting back to "WHODS" I am surprised that WHODLS is shown as a statistical machine. That name is (usually) used for an IBM program of the same name that is error and event driver for a variety of purposes. The WHODS output may be a real header.

- As an aside, CMS has a complex scheme to locate a command. When you enter a line at the terminal, CMS takes the first blank delimited word, uppercases it, and hurries it to eight characters if it's longer. Then it goes through the following search. If any step of the search finds the command, it stops there. If they all fail, you get an error message.

1. Search for an EXEC with a filetype of EXEC that is resident in storage. If it's search succeeds, the proper EXEC interpreter (there are three exec languages available) is called to interpret the file.

2. Search for a file with filetype of EXEC on any currently accessed disk. CMS uses the "standard search order" (I'll denote A-Z). The table of active (open) files is searched first. An open file may be used ahead of a file that resides on a disk earlier in the search order.

3. Search for a valid synonym (system and user supplied synonym lists) for a storage resident EXEC.

4. Search for a valid synonym for a disk resident EXEC.

5. Search for a nucleus extension command. These are storage resident commands that can replace or front end standard or user commands, or can be unrelated to standard commands and just keep residents to reduce overhead of having them multiplex lines. Some commands move themselves into nucleus extensions the first time they are called so that subsequent calls will have lower overhead.

6. Search for a command previously located into the transient area. (An 8k buffer in the nucleus.)

7. Search for a nucleus resident command
8. Search for a file with filetype MODULE on any currently accessed disk. If found, the MODULE (executable code) is located and branched to.

9. Search for a valid abbreviation or truncation of a nucleus extension. Most CMS (system supplied) commands can be abbreviated to the minimum length that is not ambiguous.

10. Search for a valid abbreviation or truncation of a command in the transient area.

11. Search for a valid abbreviation or truncation of a command resident in the nucleus.

12. Search for a valid abbreviation or truncation of any other CMS commands.

13. Search for a CP command.

14. Search for a valid abbreviation or truncation of a CP command.

- Password changing at many installations is under control of a directory maintenance or security system. In many cases, the system houses users to change their passwords at regular intervals, and some are smart enough to remember the last n passwords and will prevent you from re-using the same password over again for a while.

- No privileged commands: The system can determine the priv classes of a logged on user (there are 32 possible classes (A-Z and 0-5), only seven of which are used in standard IBM code) by examining real storage in the CPU. It takes class A or E to examine real storage. VM in concert with various security or monitoring packages can record command usage, both failed and successful. In VM proper, this monitor function is high overhead and is (usually) used only for sample intervals or when a problem is suspected. Other packages are available that would monitor commands with minimal overhead.

- In the D SENDCH output, the %E (Y) disk is usually used to store any commands that are local to this system. The %S (S) disk is usually the IBM supplied code. The %S means that if a request to get something from the S disk is issued, and it is not there, the Y disk will be searched as an extension of the S disk. The volume name (also known as the valid or valid)

VM/CMS CORRECTIONS

is not processed by CMS.

• The filename letter is the same as the disk the file resides on as accessed. If you release (logical detach) a disk and access it as a different letter, LISTFILE will then show the same files with the new letter. If you add the option "LABEL" to the LISTFILE, additional information for each file will be shown. This includes the file size, record format (fixed or variable), record length, last updated date-time, etc.

• In the list of filetypes, there are some errors. System help files have a filetype of "HELPPROX" where "PROX" is a subset of the system such as "CMS", "CP", "HEX", etc. These help files are (usually) found on the ISD disk. Under the LANGUAGEIS item, programs written in lex would normally have a filetype of EXC. LISTING files can contain anything; their distinguishing characteristic is that they usually contain printer carriage control characters as the first byte of each line. MODULE files can be any executable program, system or local. TEXT is usually used for computer output. XEDIT is the filetype used for XEDIT (the system editor) macros, which are usually written in lex or exec. The editor can create a file of any filetype. Lex's description of the filetype numbers is essentially correct. There are many ways to break the filename zero security so it should not be relied upon.

• The Passwords: The "PASS=" keyword is optional. However, be sure to pull a space after it, if you are not sure if that was a typo or a lex error. There is no VM restriction to using the same password for login and disks, and all three disk passwords can be the same. Some security systems forbid this, and it is not a good idea in any case.

• The Q DASD command shown. If you have gotten onto a privileged id, this will show the real dead that the entire system has. In this case, a "Q Virtual DASD" request will show your own disks. In the display as shown, "SYSRES" is the volume of the real disk that these minidisks are a part of. A partial listing of the real disks might look like this:

DASD 130 CP OWNED VMPCPE 0044
 DASD 154 CP SYSTEM SYSWK1 0001
 DASD 249 ATTACH TO VSEFPD 249

What this listing shows is that VMPCPE on real address 130, is "OWNED" by CP (i.e., it


contains one or more system data areas) and the currently logged on users have 44 minidisks on this pack. This can be 44 users all with the same minidisk, 44 different minidisks, or some combination. SYSWK1 is on 154, has no system data areas, and at the moment is in use by one user with one minidisk. Real address 249 is attached (indicated) to user VSEFPD as his virtual address 249.

• There is nothing in the DISMANT package that requires its use to be DISMANT. Location is because that is the default name unless the sysproc changes it during installation. The DISM LINK command can only be done if you know the password for the link made you are asking for. The disk's owner is notified when you get a link in this way. Many DISMANT comments can be locally disabled as an option during installation. Enter DISM ? for a list of commands, or DISM ? command for details on a given command.

• The system directory can have any name but usually has a filetype of DIRECT. Another common name is VMUSERS, whose lex shows a "typical" entry in USER DIRECT, ignore the lines starting with VMU01.... These are sequence numbers in columns 73-80 of the file which have been broken into 2 lines for some reason. Most likely you or the system has defaulted the size length of the terminal to 72. The two storage sizes (1M and 3M) are the default size and the maximum you can ask for (with the DDFR=870 Range command). The IPL statement says to automatically IPL Initial Program Load) the system named CMS as it goes. The DORSOL E line defines that the user's login terminal is to look like a 3215 (IBM typewriter terminal) at address 000, 009 or 01F are more commonly user console addresses. The three SPQDL statements define the virtual card reader, card punch, and line printer available to the user. The three LINK statements get access to the CMS system disks.

In conclusion, I hope that I have been able to correct most of the errors and misconceptions that I've been given you. As noted, I have omitted several things that would be dangerous for a hacker to know about VM internals. There were a lot of holes in a VM/CMS system, but most of these have been plugged by IBM or users. I hope that both Lex's article and mine have been of interest to the readership of 2500.

THESE ARE WEATHERTRAK CODES. WHEN DIALING THE WEATHERTRAK SERVICE, SIMPLY ENTER ONE OF THESE TO RECEIVE THE FORECAST FOR THAT PART OF THE WORLD. WE UNDERSTAND THERE ARE SOME HIDDEN CODES AS WELL. THE NEW YORK ACCESS NUMBER IS (212) 355-1212. TO FIND OUT THE NUMBER NEAREST YOU, CALL 800-247-3282 OR (214) 556-1122.



800-247-3282

WEATHERTRAK

WORLDWIDE WEATHER FORECASTS

AMERICA'S LARGEST WEATHER SERVICE

FOR MORE INFORMATION

CALL 800-247-3282

An Interpretation

The following article is one view of computer hackers. We'd like to say right up front that it is not ours and in fact we take exception to a good many of the facts presented. We would be most interested in hearing what the hackers of the world have to say regarding this perception of them. Please send us your feedback.

By Captain Zig

The ongoing wave of computer crime that is being reported in the media around the world shows the ease of computer system break-ins that are becoming more and more widespread. Both the technology and the society have changed since the birth of the first computer and the growth of the computer has come to the average household in the U.S.

The speed has increased while the size has shrunk. One simply has to compare the Apple or IBM personal computer to ENIAC, the first computer. ENIAC was very large and needed a small electrical sub-station to operate while the personal computer today runs on batteries or household electric. The memory in ENIAC was just about 2k compared to today's personal computers which commonly have 16 Megabytes of RAM.

All of this computing power is now in the hands of everyday persons and the equipment can be carried to anywhere in the world. In addition these people can gain access to the computer center of any major and a large number of minor computer sites. How? Through the phone lines around the world and the ability of such a vast global network to interface almost anywhere on the face of the planet. Simply put the phone and the computer are now one and the use of dial-up ports to the computer is becoming standard operating procedure. The reasons are due to the desire for distributed databases and the need for all of the information to flow over the phone networks around the world. We will now look at the issue of information flow over the phone network and how easy it is for someone to gain access to any part of the transmission.

Telecommunications and Fraud

The beginning of the formal underground phone network started in 1977 with the formation of the newsletter entitled "VPL" or

Youth International Party Line. This newsletter was structured with information on how the phone company equipment would work and ways to defeat it. This was also seen as a protest against the Vietnam war and the federal tax that was placed on phone service to help pay for the war.

The idea was to be able to place calls to others without paying any form of toll charge. This one form of toll fraud was done with the use of homemade electronic gear known to this day as the "blue box". The "box" was able to simulate the signals of the phone company switches and it could place calls as if one had the same coinlines as a regular AT&T operator.

Calls were placed over toll-free trunks such as 800 numbers. The phone company, seeing the problem, placed a tone detector on trunks looking for the distinct tone frequency of 2600 Hertz. (This tone is the signaling frequency for the long-distance trunks to disconnect but the blue box could still maintain a hold on the trunk and place calls from remote locations.)

One other interesting aspect should be mentioned—the use of a whistle that was found in the boxes of "Captain Crunch" cereal. The name "Captain Crunch" was used by the earlier phone phreak known to the phone system security force. His real name is John Draper and he was the first person who used this whistle from the cereal boxes and discovered that the toy would produce the exact same tone (2600 Hertz) that the phone system produced for the security of the trunk lines needed to make long-distance phone calls.

Other "boxes" also exist. Here is a brief list:

Blue: produces all (SP) single frequency tones and (DTMF) dual tone multi-frequency. Able to dial without incurring toll charges.

Red: able to produce coin identification tones that correspond to coins placed in a payphone (nickel, dime, or quarter).

Green: coin return. This allows the caller to return coins instead of the coins dropping into the coinbox of the payphone.

Silver: able to simulate the DTMF and have the availability of generating 1633 Hz tones are used on the American voice network (the military phone system).

Black: does not allow the correction of billing

of Computer Hacking

circuits to call. Also be used as caller party's line. This is only usable on older switches such as step by step or #2 or #5 Crossbar.

Clear: allows for calls to be placed from the new private payphones that block the phones microphone until a coin is inserted. But by using an impedance tap type of device the speech of the caller can be electronically placed in the earpiece and the conversation can proceed normally.

Orange: allows for a call to be placed to one location and then transferred to another location on a different line than the original number called. Used to find actual location of the caller from trunks by separating and isolating the call from the other line.

There are combinations to these boxes. They can be red-blue or red-green or silver-red-blue but one of the simplest ways to defeat the phone system would be to use a portable tape recorder. This would allow for the tones to be played into the mouthpiece or to use an induction coupler to enter the tones. This way there is no illegal equipment to be found and the phone phreak can do his work.

"Computing power is now in the hands of everyday persons and the equipment can be carried to anywhere in the world."

Other methods of phone fraud are now taking place due to the use of other long distance carrier networks. Carriers such as MCI and Sprint have had toll fraud problems for years and now are starting to curbing rates about toll fraud and other pertinent information. The carriers have recently formed a group that seeks information about suspected code abuse. Such information includes phone numbers dialed, called party name and address, suspected or known toll abusers, and the new problem of multi-center abuse.

Most of the known abuse is being dissected from the hacker bulletin boards but goes part numbers and access codes. Other incidents include employee use after hours or just plain fraud by using another person's code.

We will first discuss the problem of multi-carrier abuse or "weaving" through the different networks. This form of toll abuse gets its name due to the way that calls are placed to the target phone.

In the U.S., there are five major long-distance telecommunications carriers: AT&T, US Sprint, MCI, Aetna, and RC.

If a caller wanted to hide in the different networks, he could start by dialing a local PBX (Private Branch Exchange) and use the PBX as the first point of contact to place the call. Most major PBX's today have the ability to allow outsiders to gain access to the local telephone line through a switch in the PBX.

This switch gives the local dial tone and allows a call to be placed to the first local access port of one of the common carriers. The local port answers and allows a carrier or system dial tone across the line and the caller inputs the access code, area code, and number to the next target switch.

The number input is the number of a target switch in another city and allows for the caller to hide in the network of Bell and the first carrier. The second targeted switch then answers and gives a system dial tone and the process is repeated.

This progression will continue until the final target phone line is reached. Such tactics can confuse even the best telephone company attempts to trace a call. So the final product of the call is that the caller could be coming from any major port on any of the carriers. Plus the added problem of being on all carriers at the same time (in the different interconnections allows for some very interesting complications to occur.

Such access to the switch is very easy as many persons use these common carriers via long-distance calls. With the vast amount of persons who use such services, the ability to find working accounting codes is still very easy. Such codes can be found by the use of a modified "Wargames" dialer program. This particular program will call the local port of the common carrier and just like its cousin the port scanner, will scan the common carrier port with the ability to generate long-ones and "hack" out a working code that can be used for that switch. An example of a simple "Wargames" program

The Threat of

Computer Hackers

is listed. This program was written for use with an Apple II+ and a Hayes Micromodem.

The operation of the program is very slow but other faster versions of this are available to the system hacker. Other programs have been written for use by the Hayes Smartmodem and the Promethean FmModem 1200A.

(See WARGAMES listing on page 20)

It should be noted that some of the common carriers have changed the programming of their switches to only accept valid codes for the local area—that is, not to accept any other code that might work in other parts of the country. Traveling callers must call a special number and insert an additional 4-digit code after the regular authorization code.

Hacker Communications and Bulletin Boards

Some of the ways that the hackers communicate is through the use of conference calls and the underground bulletin boards. Such methods of message traffic go without change and are able to be done by the vast majority of the hackers. The hackers have the ability to place up to 30 calls to any place in the world and join all of these calls together.

Most of the calls are placed to pass information over to other hackers but can work on a problem and compare results and plan for more tactical attacks to the target system.

The logic behind the thoughts that the ability of one person to attack a system is multiplied tenfold by the others working on the same system.

Such attacks have been placed on various computer and communications systems by the hackers. One such incident took place in Los Angeles, with phone phreaks and hackers attacking the Bell System master control computers and trying to turn off all the phones in the city with the exception of the emergency circuits. This attack was for the most part successful resulting in the loss of phone service for thousands, but not complete in its goal.

But this writer's opinion about the attack is that it was very successful in showing the ability of certain persons who were able to shut down some of the phone service in the city. If such actions can be performed by persons who do not have inside information or access to the facilities, then it is a very real situation. Such attacks can be

placed to a series of phone lines or just one. Other attacks have involved the reprogramming of Bell System switches, changing the destination of 800 toll-free calls to other locations, or ringing a vast number of phones at the same time.

The phone/computer underground is still growing with the vast amount of personal computers coming into the hands of many different persons who now have a large amount of computing power at their fingertips.

Bulletin Board Systems

Bulletin boards are, as they sound, a place where persons can place information or requests for information. But in the world of the hackers, the bulletin boards are a way to pass information via computer to other hackers. These boards are setup by individuals in their homes and the users of the board call a phone number that is attached to a modem and the host computer. A bulletin board is nothing more than a place to swap information.

Such information like dial-up port numbers, logons, and passwords are common information available to the main hacker population. Other more secret information is passed in confidential messages to each other and through the use of sub-sections of the board where only a select few are able to enter.

The bulletin boards contain a wealth of information if one can gain access to them. One reason that the boards are difficult to enter is because of their security. A good rule to remember is that the under-bulletin boards have far better security than most large computer systems, and that the hackers crack out easier for their real identity. A series of checks is done that include the place of employment, the phone number, and the owner of that number.

Other security checks require that a prospective user be recommended by another user to gain access, and then the new user is granted a lower status than most users until he proves his worth in the hacker world. The chance of a law enforcement person gaining access is thereby greatly reduced. Other aspects of the security of the boards is that some of them have a clause at the sign-on that states that the board is not responsible for the information posted and that any information placed on the board is for informational purposes only and that the person

who is logging onto the system is not a member of any law enforcement agency in any way, shape, or form.

One of the methods used by the hackers to keep control and order in the hacker community is known as Tele-Trial. Tele-Trial is a court that is convened by the hackers to listen to complaints, set laws, and hand down decrees upon suspects. Such decrees can include not granting access to the boards or having someone executed electronically. Such actions have come to the public's attention with the Tele-Trial of Newsweek reporter Richard Sandia. The story with Mr. Sandia is that he wrote an article about the hacker community and the hackers did not approve of the story, so Mr. Sandia's medical card information posted on a number of bulletin boards and numerous articles delivered to his home.

Other interesting parts of this story include the distribution of his private non-published phone number and a number of death threats. Mr. Sandia then wrote an article entitled "Revenge of the Hackers" and was bombarded with another wave of abuse from the hackers. This writer's opinion is that it is better to negotiate ally with the hacker rather than to antagonize him, as he can perform your destruction in a matter of seconds and such destruction can happen at any time. And remember, the hacker can be the best prevention for computer security, sickness and that a reformer hacker can make for the best data processing security person.

In general, most of the computer bulletin boards are nothing more than a place where persons of general interest are allowed to communicate their ideas and concerns about hobbies, art, science, cars, ham radio and electronics, are at course the major reason this article has been generated—the computer/pirate underground. The boards in general have been a major problem in the control of information due to the use of the boards by what some may call "information junkies."

But the problem of the "information junkies" is one that is spanning the computer arena with all types of persons using this form of high speed communication. And one of the major contributing factors involving the computer cause is the non-education of the users in ethics. But the problem is twofold: the user must be

held accountable for his actions and the owners must secure their machines with a reasonable amount of security.

Part of the problem with the owners and of course the transmission facilities is that the carriers do not take responsibility for the security of the transmission, only that the transmission will get to the intended destination. Add to that the cost of point-to-point encryption and you get very high costs both in the equipment and in the maintenance of the system.

"The boards are considered a major nuisance to the phone companies."

The bulletin boards contain a vast amount of information at the fingertips of thousands of persons at any time. Some of the boards have the ability to have multiple users on them at one time. And the boards that we will concern ourselves with, the underground or clandestine boards, are the toughest to crack. Information on these systems can range anywhere from how to make free telephone calls to the formulation of crude plastic explosives to a person's credit and personal information. Mostly the boards are a place where the body of telecommunications and computers is placed along all other things. The hackers call it nothing more than "electronic geography." They have nothing more than a good sense of curiosity and they want to learn. So they go exploring and find things that most would consider to be trivial. Information found has been well documented and power to be embarrassing to the owners. The government has therefore given both the Secret Service and the FBI the job of investigating all computer crimes. This includes the investigation of the underground bulletin boards.

The boards are considered a major nuisance to the phone companies, but are only considered a small threat to the computer owner. But they still produce good copy for the printing paper and evening news. The general public thinks that the hackers are wonder site able to launch a nuclear missile in any direction who can invade any

(Continued on next page)

The Hacker Threat

computer system out there. They hear that a computer that belongs to the U.S. government in a nuclear research facility has been "tapped" by the hackers, or that there is a possibility of the hackers controlling satellites and moving them out of their assigned orbits. Granted, they did not move the bird, but they did gain access to the rotation control for the satellite.

And it was stated that the information needed to do such things was found on an underground bulletin board. That might be true, but information that is far more valuable to people on earth is being posted on the boards. And this information comes from the trash can or from insiders who have become disgruntled or just from plain old research—looking for publicly available sources. Some of these public sources constitute users' manuals and system documentation.

Another interesting fact about the boards is

that they contain a group of sub-sections that include subjects on telecommunications, software piracy, and cracking of software protection systems, computer systems overviews and how different systems work, and ways around the system security features. Some bulletin boards also contain page after page of dial-ups to major computers around the country. These include all of the Fortune 500 companies and a large amount of military systems. So to the persons who state that the bulletin boards are not a problem, I believe that they have not been on any of the major underground boards and therefore should not make such rash statements. As to the overall message that a bulletin board can cause, the final cost has yet to be determined. The boards allow for the transmission of information to a large group of persons. What the person who gets this information does with it is another story.



FIGURE 1
Ripple



FIGURE 2
Clock

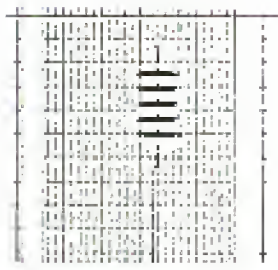


FIGURE 3
Quarter

0 1 second

```

1  REM "MARGAMES DIALER PROGRAM" FILE MUST BE OPEN FIRST
5  INPUT "NUMBER TO START" N
10  DG=CHR$(44) : QS=CHR$(17) : Z$=CHR$(26)
15  FOR I=N TO 9999
20  M$="0000" + STR$(I) : N$="5E7" + RIGHT$(M$,4)
25  PRINT D$ "PR42"
30  PRINT Q$ " " " R$
35  IF PEEK(16581) 1/4 120 THEN 1990
40  PRINT D$ " PR40 "
45  PRINT D$ " APPEND DIALER 567 "
50  PRINT D$ " WRITE DIALER 567 "
55  PRINT M$
60  PRINT D$ " CLOSE DIALER 567 "
65  PRINT Q$ " CHR$(26)
70  REM HANG UP AND BE SURE THAT YOU DID
75  PRINT D$ " DRPD "
80  PRINT D$ " PR#2 "PRINT D$PRINT 25
85  FOR J=1 TO 600 : A=-1 : NEXT
90  NEXT
    
```

THESE OSCILLOSCOPE READINGS CAME FROM THE NEW JERSEY BELL INVESTIGATION OF THE PRIVATE SECTOR 2600 BULLETIN BOARD SYSTEM BACK IN 1985. THEY ARE MEANT TO PROVE THAT OUR SYSTEM OPERATOR INTENDED TO DECEASE THE PHONE COMPANY BY USING HIS COMPUTER TO Imitate THE SOUND OF COINS DROPPING INTO A PAYPHONE. THEY DON'T EXPLAIN HOW HE WOULD HAVE DRAGGED HIS NON-PORTABLE COMPUTER OUTSIDE TO A PAYPHONE TO ACCOMPLISH THIS, BUT THEY DO SAY LOTS OF OTHER INTRIGUING THINGS AND WE'VE REPRODUCED ONE OF THE LETTERS FROM THESE TECHNOLOGICAL GENIUSES FOR YOUR ENJOYMENT ON THE FOLLOWING TWO PAGES.

FROM THE 2600 FILES

RFI
Communications
Research

Telephone Network Security
Electronic Bell Fraud - Blue
Investigation of Evidence
File-3

August 21, 1988

Mr. R. N. Poyrka
Security Administration
New Jersey Bell
550 Broad Street
5th Floor
Newark, NJ 07101
Dear Mr. Poyrka:

I have completed production of the floppy disk you thought to be the correct Security Administration of Bell Communications Research, and have, New Jersey of July 23, 1988. It refers to a New Jersey Bell Investigation 26-0003 involving Thomas Stone, resident 88000 Boulder Road, Newark, New Jersey.

The 5 1/4 inch floppy disk carries the following material:
- Disk Number 041
- TEE CAT'S HEAD
- CAT NUMBER 2.71
- 26000 MESSAGE
- M0311

The name "CAT 1/22" also appeared on the label end of the disk at my examination I added my mark "2600-001 7/22/88."

The disk was loaded into an Apple II computer and the contents displayed on the screen (Table I). The program "The Cat's Head" refers to electronic signals, and the program instructions were listed (Table II). The purpose of the program is to produce a variety of tones used in the telephone system, including the signals of a Touch-Tone (TTS), the 1600Hz tone (TTS signal) and the tones of the 2-out-of-6 multiplexing key pulsing (TTS) code used in the long distance telephone network, and the coin deposit signals produced by coin telephone coin slot when coin are deposited. A tone generator producing 1600Hz and the TTS signals reproduced the ten digits and the control signals for and ST can be used to redial long distance calls to any destination with depressed Billing equipment. Such a generator is commonly called a "blue box." A signal generator that simulates coin deposits signals is called a "red box."

On August 13, 1988, Theodore Michael Greenberg, 8001 241-4124, New Jersey, brought the following equipment to RFI Laboratory:
- An Apple IIe personal computer, SN 1201187 equipped with
- Revision 02000000000000000000, 41031
- Hard Disk, Xerox Mod. 8110P, SN 4-0794
- Floppy Disk Drive, A4100031, SN 1045010, and 1185312

- 2 -

Paroleman Greenberg loaded the program "The Cat's Head" (see the 5 1/4 inch floppy disk into the computer and pressed the letter D on the keyboard to select the disk status of the program. Structure of the program was shown on the monitor screen. The audio output was fed to signal analyzing equipment which produced a waveform (see Table III) showing 215 Analyze the "Good" digital storage oscilloscope, model 4600C used with a Sony Brush 280 oscilloscope.

Table III shows the appearance of the screen. Pressing the letter F returns the Touch-Tone tone. Paroleman Greenberg entered the sequence of digits 1 through 0, followed by * and #. The computer produced tones which were analyzed by the signal frequency analyzer. Its printed output is shown in Table IV. The signals generated are those produced by a telephone set with push-button dial.

Next, Paroleman Greenberg pressed the letter R on the dialer key. The multiplexing code was then entered the sequence 1 through 0 followed by N, T, and J. Table V shows the analyzer output which identifies the signals as the 1600 Hz tone signaling code.

Paroleman Greenberg then loaded and ran the same program from hard disk, repeating the procedure described above. The results of the measurements are shown in Tables VI and VII. They correspond to the results shown in Tables IV and V.

Finally, Paroleman Greenberg pressed letters L, M, & N in succession. The computer produced new, red, and blue tone bursts, respectively. Figures 1 through 3 are representations of these tone bursts captured by the oscilloscope and back recorder. Their duration and spacing coincide the format to indicate coin deposit signals.

Paroleman Greenberg managed to control of the Apple computer and associated equipment throughout the run and left with all equipment he had brought after the measurements were completed.

The floppy disk you thought to be returned to you herewith.

Approximately 15 man-hours were required to perform this analysis.

Very truly yours,
Theodore M. Greenberg
Theodore M. Greenberg
Member of Technical Staff
Research Security

RFI-02000000000000000000-21
RFI-02000000000000000000-21
41031
Green Statement
Pages 1 through 7
Tables 1 through VII

More Secrets

Dear 2600:

Something that may interest readers and raise a few questions about the US government is the National Coordinating Center located in Arlington, Virginia. This is part of the Defense Communications Agency and is operated by the Pentagon. Its stated purpose is to make available all civilian communication facilities in the time of a national emergency to the Department of Defense. Its staff includes representatives of 12 of the United States' largest communications companies, including MCI, Comsat, ITT, GTE, and of course, AT&T, as well as members of various federal agencies.

The President's car, in times of what's termed a "606 Emergency", take control of any communications facilities if he thinks it is necessary to the "national defense". This power was given by the Communications Act of 1934, and the NCC, which was created in 1984, is the place that would allow this to happen.

If readers want more information on the NCC and some of the actions that make it more threatening than its intended purpose, there was an article written in a mid-1987 issue of *Omnif* entitled "National Guard". I can't leave the exact date because I don't have it. But this is a topic that is well worth informing yourself of.

Hopefully, awareness will grow about the potential for abuse that comes from the capability of controlling much of the public's sources of information, as our political system becomes increasingly intertwined with new technologies and their applications. 2600 should be praised for its efforts in educating people in this field of thought.

Encouraging Words

Dear 2600:

I figured you might get some cynics writing in saying they don't like the new quarterly format. So I thought I'd write and say that this new format looks just great to me. Keep up the good work!

A Friend in Texas

Obviously you had to have written this letter before this issue was ever published. So how you were able to tell it would look so nice is beyond us. We have to say, however, that we're pretty pleased with the way it came out too.

Still More Secrets

Dear 2600:

I am not a subscriber, but I was wondering if you could give me some info on the following things:

First, have you heard of a system called "Terec"? It's based in Sacramento, California and is massive! The memory as calculated in megabytes is as follows: 10E+100-10E+100+10E+50. As far as I know it is used by military for a temporary storage. An example of a logon would be: Password, madness, ID: 25813, security level code: mad 532, security level code 2, mess 532. (Note: these numbers change after each login randomly.) Security level codes are three alpha and three numbers or three alpha, two number, and one more alpha.

The second system logs on saying it is "Mashles BBS" and operates like a regular (but weird) BBS. The following commands are available: A-answer call, B=??, C=??, D=??, E=mail, S=send letter, R=receive letter, M=make call, Q=quit. However, if you mess around with it enough, you'll get asked for a password. After getting through 15 passwords, 20 identification numbers, and 62 levels of access, the system

tells you it is the "Military Operations Unit System" and then the Artificial Intelligence kicks in. Then from there if you were to tell it to "launch missile", it will ask you what type of missile, target, from where, etc. Then it will start a countdown. I stopped it before zero but I was wondering, could someone really launch the missile? Isn't there a human factor involved?

If you know about these systems, or know anyone who does, please write me some notes on them. Terec traces all calls coming in, and both systems have artificial intelligence to some extent. Terec accepts ROM dumps but MOUS doesn't. MOUS doesn't trace or anything and the two systems are linked. (You will not find out by using them—I didn't.) But if you get busted if did, they will usually just tell you to stop calling.

Also, have you guys figured out how NASA ciphers all their shit? I can get in but I can't read anything.

First of all, we appreciate your stopping the countdown. Second, since your letter didn't bear a Yale postmark, we assume it's serious. Somehow you managed to get through 62 levels of access to the massive hawking program and you're asking us if we know anything about these systems? Either this is an incredible case of exaggeration or it's another test of our patriotism (with 2600 help overthrow the government or will we run and tell the good guys about the bad guys without ever suspecting that they're really one and the same, etc.) Or the old chance that what you're saying is true, you're better off showing us what these systems can do rather than waiting until it's too late or telling the wrong person. Anonymity guaranteed.

A Very Special Number

Dear 2600:

Now that Jerry Falwell has disconnected his 800 number, callers may wish to dial the National Rifle Association at 800-368-5714. They only answer between 8:30 and 5 Eastern Time, Monday through Friday. But the firm that does their telemarketing can be reached 24 hours a day at 800-535-2200.

What a wonderful public service ...

Tales of Hackers

Dear 2600:

Enclosed is another newspaper article about someone hacking MCI codes and getting caught after the calls were traced back to his apartment. To top it off, he also got busted for the pot plants on his balcony. Some people never learn from other people's mistakes and seem to have to find out first hand.

I found a goony in An Introduction to

Police suspect UP hacker stole long-distance codes

A police investigation is under way to determine whether a hacker who stole long-distance codes from the University of Pennsylvania (UP) was the same person who stole codes from the University of California, San Diego (UCSD) last year. The investigation is being led by the FBI's New York office, which has been investigating the UP hacker since last fall. The UP hacker, who is believed to be a student at the university, is suspected of stealing long-distance codes from the university's computer system. The UCSD hacker, who is believed to be a former student at the university, is suspected of stealing long-distance codes from the university's computer system. The FBI is currently investigating the possibility that the two hackers are the same person.

LETTERS OF THE SPRING

Operating Systems published by Addison-Wesley, a short PL/I program to lock up a computer running under OS/360.

REVENGE: PROCEDURE OPTIONS (MAIN TASK):

WAITEVENT);

END REVENGE;

Supposedly this makes the computer wait for something that won't happen and tie up the system. I have not had an opportunity to test it myself.

The Hooded Claw

Advice Wanted

Dear 2600:

I have recently subscribed to your magazine because I am starting an "on call" personnel business, screening potential employees.

Frankly, I am quite new to computers, but am determined to get a set-up which will enable me to conduct business from my home.

I am wondering if there are any people around who could help me in this regard by telling me what software to purchase and how to gain access to public records in all states, for background check purposes.

Some of the types of things I want to access are county records, federal court records, worker's comp records, and driver records.

The process through the mail (which most governmental agencies make available) is very slow.

I am also interested in obtaining any other personal background information (credit history, military records, assets).

If there is a publication with access codes, etc., please let me know about it, because I really want to get this business going.

Responds as if you want to bypass the system and do things efficiently. Often, this means bending or even breaking the laws. You won't get anywhere if

you depend on publications that print access codes. You want exclusive access to your sources. If you have to share this access with anyone who can get their hands on a publication, it just won't be effective. We distribute information but there is a limit to how far we can go. If we were to print passwords or codes (despite the fact that it's illegal), so many people would use them that they would soon get shut off or monitored very closely. For that kind of information and the kind we suspect you're after, you need to make personal contacts - through the mail, on the phone, on bulletin boards, or on the street. You'll have to use your instincts insofar as who you trust and what information appears valid. If we've misread your question and you actually want to do this by the book, we're sure it's possible. Simply go through the agencies involved. But, as you've already noted, that tends to be slow, and quite often expensive.

Of Phones and Politics

Dear 2600:

The importance of the telephone in modern life became apparent in the recent New Hampshire Primary Debate of the Democratic party. The first question asked by the moderator was directed at Senator Paul Simon in reference to the Senator's proposal to put free telephones in the homes of those who could not afford them. He would place a two percent tax on long distance charges to pay for this program. Bruce Babbit attempted to discredit the proposal by challenging Simon to address the broader issue of the deficit. Gary Hart tried to ignore the subject altogether but Representative Albert Gore showed himself to be the most knowledgeable "telemom enthusiast" seeking the nomination by attacking the Reagan administration's policy of local "access fees" to

subsidize long distance service for big businesses. Gore also stressed the need of making telephones affordable to the widest base of people possible. Telecom may be on the agenda, but we're waiting for a candidate who will support 2600's campaign against touch tone fees!

Skinhead, Steve and The Boy

You'll be waiting a long time unless you start telling them about it. Politicians know rightfully little about high tech. They need people like us to explain it to them. A well worded letter to your elected official explaining why the touch tone fee is a ripoff may yield surprising results. What have you got to lose? By the way, if any readers need the focus on the touch tone fee, we suggest thumbing through our 1987 issues.

More on the 8038

Dear 2600:

Not to drag the 8038 issue into the ground or anything, but...

The IC8038 is still in production and fairly easy to get if you just look around a bit.

For complete data, call 14081 996-6000 and ask to be sent the 1987 Component Data Catalog.

Although you all have no control over what people advertise in your 2600 Marketplace, \$7.50 for one 8038 is ridiculous!

REMOB Hunting

Dear 2600:

The attached is from William Poundstone's *Bigger Secrets*. I'm interested in the reference to "REMOB" on page 84 and on other surveillance techniques.

The ultimate in phone spying is REMOB, remote observation. The phone company is said to have certain secret numbers—one is in Iowa—that can be used for listening in on other

numbers. You call the REMOB number with a touch tone phone, then punch in two access codes and the phone number you want to tap—which can be anywhere in the country. The tapping is done by a sophisticated technique that does not create a telltale click, hum, or beep. It's all done automatically, without an operator, and anyone knowing the number and access codes can spy on anyone anywhere.

I don't recall ever seeing "REMOB" addressed in the newsletter. Can anyone add to it?

MH

Uniondale, NY

We have yet to see specific evidence of a working REMOB. But we do believe their existence is possible, certainly from a technical view. It's doubtful that one system could spy on numbers across the country because of the many different systems still in use. If and when all of the phone networks become integrated, such a concept will be very possible. For now, we will offer a reward of \$100 for the first person who comes forward with a working residential REMOB. That ought to settle matters, one way or the other.

The Global Village

Dear 2600:

In the October 1987 issue of 2600, you wrote about how people from all over the world wish to run electronic bulletin board systems under the name of 2600 Magazine.

Here are my ideas: enlist the aid of hackers and phreaks from all over the world to write a combined version of Diversi-DIAL and Fido for all major brands of personal computers. Second, since this is supposed to be like a global village, setting of telecommunications hobbyists for use Communications Revolution, why not substitute it for our own after Dr. Isaac Asimov's *Foundation* (see page 100).

LETTERS

(Continued from previous page)

Foundation novel?

Because what you are trying to do is gather people and data together to create a digital sanctuary for ensuring freedom of speech, especially now since advancing technology allows us to use that basic freedom to reach more people than ever before. That is sort of what the Foundation novel was about.

I hope the hackers and phreaks of the world are willing to write this much needed BBS software, because too many of us are kept apart by the telephone systems of our countries. For if we really wish to learn and finally control, we need common places where we can go to draw on and then expand our knowledge.

The NATO Association

We need as many methods and channels of reaching people around the globe as our imaginations permit. The computer/telecommunications revolution can be mankind's salvation or doom. We're helping to make that decision.

Got a letter for us? Send it to: 2600 Letters, PO Box 99, Middle Island, NY 11953.

Attention Readers!

2600 is always looking for information that we can pass on to you. Whether it is an article, data, or an interesting news item—if you have something to offer, send it to us!

Remember, much of 2600

is written by YOU, our readers.

NOTE: WE WILL ONLY PRINT A BRIEF, IF SPECIFICALLY REQUESTED.

Call our office or BBS's to arrange an upload. Send US mail to

2600 Editorial Dept.

Box 99

Middle Island, NY 11953-0099

(516) 751-2600

AT&T ALLIANCE

Teleconferencing Services

TO SET UP CALL YOURSELF

Dial 0 + 700 + 456-1000 on any touch tone phone. Also coding and set up when to:

1. Enter the total number of locations, including yours.

2. Dial the local number. Listen. Speak. Then, when you hear the tone, dial the local number.

3. Repeat step 2 for remaining locations. Then, when you hear the tone, dial the local number.

NOTE: You will be billed for the cost of the call. Please refer to the AT&T Billing Manual for more information.

GENERAL TIPS

During set up: During the call

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

Dial #1 to answer. Dial #1 to

PLEASE RETURN THIS FORM WITH PAYMENT TO ENSURE PROPER CREDIT

RCT CORPORATION
P. O. BOX 20401
ROCHESTER, NEW YORK 14602

MAKE CHECK PAYABLE TO:



ACCOUNT NO. 002944
BILL DATE 02/26/88
PAYMENT BY 03/25/88
PAY THIS AMOUNT 0.06
AMOUNT ENCLOSURE

1

RCT CORPORATION • 523 METRO PARK • ROCHESTER, NEW YORK 14626 • CUSTOMER SERVICE 1-800-891-2713

CHECK: POSTER WE GOT A FOUR-PAGE BILL FROM RCT FOR OUR SERVICE. THE BILL FROM RCT WAS OVER A YEAR FROM ESTABLISHMENT. THEY GOT A BILL TO FIND THE END POINT WHERE THE DISCONNECT IS OUR RESPONSIBILITY. WE'RE MENTIONING THE FACT THAT WE ONLY GOT FOUR PAGES FROM RCT. WE'RE MENTIONING THE FACT THAT WE ONLY GOT FOUR PAGES FROM RCT.

ROLM Phone System

The next time you find yourself cursing and swearing at the telephone because it's gotten too complicated and bureaucratic lately, keep in mind that it could be worse. You could be at the State University of New York at Stony Brook.

Being relatively close to our offices, we've been able to follow this story rather closely. We don't doubt that similar escapades are occurring all over the country and will continue to do so in the future. We'll certainly love to hear about them.

In The Beginning

Up until 1967, using the telephones was very simple. The phone system at Stony Brook was a Centrex operated by New York Telephone. Everyone on the campus used the 246 exchange. To reach the main switchboard, you would dial (516) 246-5000 from the outside world. To reach the old, antiquated UNIVAC computer system, you'd dial (516) 246-5000 from off campus or 8-8000 from on campus.

Most of the phones were rotary dial. Callers simply dialed 9 to get outside access unless their lines were restricted to on-campus only.

It wasn't the best of systems by far. It was slow and old fashioned. But it did work. And most people had little trouble understanding it. Eventually, though, everyone knew that there would have to be a change.

In 1986, the university began installing a brand new phone sys-

tem: the ROLM CBX II 9000. This would be the system to bring the campus into the information age, with useful features and high speed data capabilities.

There would be a transitional period. The 246 exchange would be phased out over a period of two years and the 632 exchange would be created. The neighboring University Hospital (using the 444 exchange) would switch from its Northern Telecom SL-1 switch to the ROLM system in 1987. The entire campus, student dormitories the last to go, would be cut over to the ROLM system by Fall 1988.

But it didn't work out in quite that way.

Of course, no one in their right mind would expect such a project to be 100 percent on schedule. But not even the pessimistic were able to predict the incredible range of problems and hiccups that the ROLM telephone system would bring to Stony Brook.

To start with, a certain amount of "culture shock" has to be expected whenever something new is introduced. This is why it is essential for something like a phone system to be easy to grasp as well as logical. Unfortunately, the ROLM system has been neither, at least not for most average people.

The first sign of trouble came in the form of a memo from the Communications Department at the university. All answering machines, modems, speaker-phones, and anything else that

Creates a Nightmare

hooked into a telephone would not work on the new system—at least not without an expensive digital-to-analog conversion device. So everybody had to conform to the same system.

Modem users had to obtain a special device that hooked their computer into the "modem pool". All data calls had to be placed through the modem pool and no longer from individual lines. Incoming calls were more complicated. Callers could no longer just dial the phone number of the computer they wanted. They would have to dial 632-8000 to connect to the modem pool and then enter another five-digit number before being connected.

Instead of using answering machines, everyone was forced to use the ROLM Personal System.

"It's reached the point where I dread hearing the phone ring. I'd say at least a third of the time something goes wrong somewhere along the line."

a voice message system that is fairly flexible, but not a true replacement for one's own answering machine. Messages do get lost, mailboxes get full much faster than answering machine tapes, the system is easy to break into mainly due to three-digit default passwords and the fact

that Phonemail provides a fairly complete listing of mailbox extensions after hearing a few stars from a touch tone phone. Plus the very simple fact that it just isn't tangible.

To leave a message for someone, the caller had to either dial the number that was hooked into Phonemail or a number that forwarded to Phonemail. Or they could dial 632-6601 and choose the five-digit extension they wanted to leave a message for. To retrieve messages, the Phonemail subscriber would dial 632-6600, enter his extension (or name), and password. Not quite the same as pushing a button on an answering machine. The advantage of course is that messages could be heard from any location. The disadvantage is that they could be heard by any person.

More Problems

On most key phones (office phones with several line buttons), you would answer the phone by picking up the receiver and punching in the ringing line button. That is known as a logical, not to mention traditional, way of doing things. Why the ROLM people chose to abandon this simple way of answering the phone is completely beyond us. As office workers and professors throughout the campus have found out, picking up the phone the "old" way will immediately disconnect the caller.

It is true that the university

(continued on next page)

ROLM System Horrors

(continued from previous page)

offered training classes on how to use the new phones where this change in phone logic was emphatically pointed out. And it is true that the 88-page phone manual made note of the fact on page 4. But a great deal of people still thought they could answer phones without reading manuals or going to classes. The reality of the matter was that thousands of potential phone-answersons would have to be trained and retrained. And even then, mistakes would be common.

"It's reached the point where I dread hearing the phone ring," an administrative office worker says. "I'd say at least a third of the time something goes wrong somewhere along the line. And a lot of the callers get angry. Who can blame them?"

New telephone numbers were assigned on the ROLM system with little or no input from the phone users. Instead of assigning easy-to-remember numbers for commonly dialed offices and services, it was, with few exceptions, done sequentially—either alphabetically or by location. For instance, campus information used to be reachable at 246-3636. Now, everyone must remember 632-6830.

Under the old system, the campus radio station was able to provide a school closing hotline. Callers would dial a number and hear a listing of schools that were closed because of adverse weather. Only one caller at a time could access this information.

Under the new system, this service had to be switched to the Phonemail system. But because ROLM had never installed any kind of a filter on Phonemail, the entire system would get tied up whenever more than ten callers dialed in. No one could get into their voice mailboxes or leave messages. So the school closing hotline, an undeniably valuable service, was shut down by the university.

Even the university's main switchboard was affected by this. They could no longer put a recording on when the switchboard was closed because the same problem of overcrowding would occur. At pressing, after-hours callers to either the old 246-5000 main switchboard number or the new 689-6000 main switchboard number got a nonsensical Phonemail recording that even gives away a "secret" internal extension number of the main switchboard, as well as the hidden ID of their Phonemail account. Terminiology matches on.

Another change everyone was forced to live with was the denial of access to outside operators. Because the new system uses its lines to make outside calls, operators have no way of verifying the actual telephone number the caller is dialing from. Access to New York Telephone and AT&T operators was therefore cut off.

This meant no third party, collect, or otherwise operator-assisted calls were possible. It also

NEW DIALING INSTRUCTIONS

On April 15th the final phase of the ROLM Telephone System installation will begin. This will include the replacement of all Campus 1000's, Campus 10000's, Campus 2000's, Main Campus, and the 8000's. The following instructions should be read carefully by all students, faculty, and staff. The ROLM system will be installed on April 15th. The ROLM system will be installed on April 15th. The ROLM system will be installed on April 15th.

Area Telephone System Users
The University of Stony Brook Telephone System will remain on the old system. To call a local number, dial 301, followed by the area code, and the number. To call a long distance number, dial 301, followed by the area code, and the number. To call a collect number, dial 301, followed by the area code, and the number. To call a payphone number, dial 301, followed by the area code, and the number.

On Campus Dialing
To call a local number, dial 301, followed by the area code, and the number. To call a long distance number, dial 301, followed by the area code, and the number. To call a collect number, dial 301, followed by the area code, and the number. To call a payphone number, dial 301, followed by the area code, and the number.

Emergency
To call 911, dial 301, followed by the area code, and 911. To call the police, dial 301, followed by the area code, and 3030. To call the fire department, dial 301, followed by the area code, and 3030. To call the ambulance, dial 301, followed by the area code, and 3030.

These Incredible Instructions Appeared in the State University of New York at Stony Brook's Telephone Directory as the New ROLM System Was Being Installed. We Challenge Any of Our Readers to Show Us an Easier Way to Summon an Ambulance than Dialing 312-2-8888.

HEALTH SCIENCES CENTER AND UNIVERSITY HOSPITAL

The following instructions should be read carefully by all students, faculty, and staff. The ROLM system will be installed on April 15th. The ROLM system will be installed on April 15th. The ROLM system will be installed on April 15th.

Area Telephone System Users
The University of Stony Brook Telephone System will remain on the old system. To call a local number, dial 301, followed by the area code, and the number. To call a long distance number, dial 301, followed by the area code, and the number. To call a collect number, dial 301, followed by the area code, and the number. To call a payphone number, dial 301, followed by the area code, and the number.

On Campus Dialing
To call a local number, dial 301, followed by the area code, and the number. To call a long distance number, dial 301, followed by the area code, and the number. To call a collect number, dial 301, followed by the area code, and the number. To call a payphone number, dial 301, followed by the area code, and the number.

Emergency
To call 911, dial 301, followed by the area code, and 911. To call the police, dial 301, followed by the area code, and 3030. To call the fire department, dial 301, followed by the area code, and 3030. To call the ambulance, dial 301, followed by the area code, and 3030.

These Incredible Instructions Appeared in the State University of New York at Stony Brook's Telephone Directory as the New ROLM System Was Being Installed. We Challenge Any of Our Readers to Show Us an Easier Way to Summon an Ambulance than Dialing 312-2-8888.

DIALING INSTRUCTIONS ■ 6

The ROLM College Campus

(Continued from page 32)

meant that non-direct-dialable overseas calls were impossible. Technically, the campus operator can hook callers up to a real operator, but is reluctant to do this most of the time. Besides, campus operators are gone at 4:30 pm and all of the weekend. Since Stony Brook consists of a very large number of foreign students who need to call strange countries at weird hours, we can only hope that when the dormitories are hooked in later this year, operators will be accessible. If something isn't changed by then, an incredible hardship will face such students. The only possible way to make such calls will be by dropping money in a payphone (calls cannot be charged to the 632 exchange) or by finding another number to charge the call to from a pay-phone.

But operators are only one of the basic services that have been denied to users of Stony Brook's ROLM system. The 976 dial-it exchange is unreachable from any phone. This is becoming common in institutions, but the fact remains that there are many legitimate uses for dial-it services. A simple task like setting a clock is now very time consuming and frustrating. And when the dormitories are cut over, will all students be prohibited from dialing Sportsphones or their horoscopes from their own phones?

Equal access rights have been all but denied to the phone users. The system will not allow you to

place a call through a carrier of choice unless the 950 exchange is used, in which case the call can't be billed to the originating number. And the 950 exchange is unreachable except on lines with long distance access. This is stupid, since 950 is toll-free and allows callers to charge calls to their own accounts. Toll-free 800 numbers, on the other hand, are accessible on all outside lines. It seems obvious that the programmers don't understand the concept of 950 numbers. As a result, the end users are inconvenienced.

Some local exchanges are also unreachable because the people who program the switch haven't gotten around to entering them, despite numerous reminders and requests from users. The 474, 476, and 656 exchanges have all been around for many months now. Without a long distance line, you cannot access these local exchanges.

Nightmares

But far and away the worst aspect of the ROLM CBX at Stony Brook is the outages. Despite the fact that they're not supposed to happen, they do. Quite frequently. Sometimes only for a couple of seconds, sometimes for a couple of hours.

Under the old Centrex, you could always get a dial tone. Even if the power went out, the phone lines were there. Now, whenever something goes wrong, everything is frozen. No incoming calls. No outgoing calls. No on-campus

Incomprehensible Bureaucratic Mess

calls. No data communications (remember, everything has to go through the modem pool). No intercoms (the phone system now incorporates those, too). No answering machines (thanks to Phonemail). Complete and total integration. Complete and total paralysis.

Recently, University Hospital had a serious outage. Nobody was able to dial anything. Eventually, it not already, this system will claim some eyes.

Occasionally, in the words of a ROLM switchroom employee, preventative maintenance requires the phone system to come down. And that is where the engineering and human perspectives of telephones come into conflict. Phone systems cannot be treated as if they were large, multi-user computer systems that occasionally crash. Phones are different—they are vital and personal.

Uselessness

To this day, the vast majority of phone users do not use most of the features of the phone system, either because they have no idea of how to use them or because they have no desire to. As a result, most of the phones have at least four completely useless buttons on them. If the user wants a different configuration of buttons incorporating those features, that they can use, they're told that it's "not possible". That's not what ROLM or the university said before the system was installed. ROLM itself has inhibited the potential of its own

system by discouraging user programming.

The most useful feature on the system is the Repertory Dialing button. It's like a speed dial button except it can be programmed to incorporate all kinds of other features. In other words, one "repertoir" button can duplicate any other feature button or combine several features, or do something entirely different. A few of these buttons would allow for great flexibility for users. But getting more than one of them is completely impossible. A potentially positive application is therefore turned into yet more frustration.

Call picking is another feature that could be useful for some. If a phone is ringing and you can't get to it, you simply hit the "pick" button and enter the extension that's ringing. It will then magically appear on your line. The only problem with this is that there's no stopping it! As long as someone knows the number of a ringing extension, they can divert it to their line. Call picking can also be used to snatch calls that are on hold, although that "feature" isn't documented. This kind of a feature works fine in offices where everyone is presumably working towards the same goal. But on a college campus of more than 20,000 people, this "kidnap" ability is ill-considered and dangerous.

Although it has lots of unused potential, the ROLM CBX II 5000 is, by and large, poorly designed for offices. A simple feature like

(Continued on next page)

ROLM System Horrors

(continued from previous page)
 distinctive ringing is common in today's phone systems; you'll even find it in cheap two-line phones at Radio Shack. But not here. You can change the way the ring sounds, but all lines will sound exactly the same on the same multi-line phone. You can't even turn one line off and leave another on! The only way to have access

NOTE

Once you have lifted the receiver to answer a call, do not press the line button. Doing so will disconnect the call.

to all of the lines in your office and have distinctive ringing for each is to have a different instrument for each line. Truly brilliant.

For those that have realized that ROLM doesn't provide all the answers and causes a good deal of the problems, the university administration bureaucratically tor-bids users from installing their own systems or even individual phone lines. This creates an inconvenience--and a danger.

As we said earlier, what's happened at Stony Brook is happening in other places. It represents something scary about our emerging technology. While great things are possible, so are big problems. And nothing will lead to disaster quicker than an unwillingness to prepare for those worst-case sce-

narios. It is vital not to be dependent on any form of technology because when it fails, you will be crippled. This is a very basic rule that is being followed less and less. How many of us have lost hours of work into thin air because of a computer glitch? Something as crude as a printed copy of our work could have saved us so much trouble. Crude backups must also exist on our new phone systems so that when they do unpredictable things, we'll be able to get access to the basics, like an outside dialtone.

What's particularly unfortunate in the Stony Brook/ROLM scenario is the pairing of a huge corporation with a huge bureaucracy. A simple human being is no match for this ugly combination. He is thus pushed around and forced to alter his way of doing things because that is the way it has been decreed. In reality, he should be the one running the show.

Clearly, more user participation is essential, both in the choosing of an institutional phone system and in its operations. These systems must be designed based on comments and suggestions from the ordinary users, not just those who understand all the computer/telephone jargon. The corporations and the institutions have got to start listening and acting swiftly to correct mistakes and inadequate facilities.

Otherwise, an increasing number of us will become disconnected altogether.

The big story in the phone industry lately seems to be the most recent consumer craze: call blocking. This is basically a service that shuts off access to certain dial-in numbers, largely a response to the pornographic services being offered on many of those numbers.

In Idaho, the plan has been approved for customers connected to exchanges equipped with digital switches. They will be able to block calls to the 976, 430, and 499 exchanges, as well as calls to the 900 nationwide numbers. For the first 90 days, there won't be a charge.

In New York, the plan is to take effect in April. Customers will be able to block access to the 550 and, or 970 exchanges without paying a fee for the first 90 days. After that, they'll have to pay between \$5 and \$10. The 550 exchange currently handles group-selling services, also known as anonymous conference lines. The 970 exchange will be altered to house primarily adult-oriented messages. The 976 exchange would not be blocked but would not contain pornographic material, as it does now.

New York Telephone is also planning to expand its dial-in network (remember, last year, they operated 59 message lines). They're now planning on expanding that to over 300.

Meanwhile, the House of Representatives has voted against an outright ban on so-called "dial-a-port" telephone messages. By a vote of 200 to 179, the House decided it would be better for such calls to be blocked technically rather than banned altogether. Such a banning could be interpreted as a violation of freedom of speech.

U.S. West has established a separate 960 exchange for adult messages rather than have them on the 976 exchange. They also won't provide billing and collection for the 960 service, although they'll supply vendors with the information necessary to do their own

billing.

Customers in that region will also be able to block other exchanges.

Bell Atlantic is creating a separate exchange for conference services and adult messages. But they've decided to block all calls to that exchange unless the customer requests otherwise. This "unblocking" service will be free. It will be interesting to see how many people will "register" their pornographic calls with the phone company.

AT&T is eliminating financial incentives to vendors who lease its dial-a-service lines in the 900 area code. This is seen as an attempt to eliminate the pornographic services that are found there.

Throughout all of this, everyone seems agreed upon one point: Phone companies cannot refuse to transmit messages regardless of their content. The constitutional guarantee of free speech does not allow for this. When will we start to apply this to computers, specifically computer bulletin boards? *

Recently, the Supreme Court ruled that student newspapers could be censored by school administrators without interfering with anyone's freedom of speech. We're dazed if we can figure out how this is possible. We also think computer hackers and technically literate people can lend a valuable hand in challenging this dangerous precedent.

How many of us have access to computers and printers these days? You know, not unthinkingly a growing number. Every kid going to school today that has a computer and a printer in his home or even in his school is a potential newspaper editor. Even something as crude as a one page dot matrix printer can be considered a newsletter. Because of this, it's suddenly incredibly easy to put out a newsletter and distribute it in school. And what can be done about it? Very little, short of martial law.

(continued on next page)

HAPPENINGS

(Continued from previous page)

In this way, we can use technology to express ourselves openly and keep from being manipulated and silenced. If you think you're capable of publishing such a newsletter, do it. Encourage others to join you or compete with you. Offer to use your computer to help give a voice to others that may not have computer access. You don't need school money anymore. You don't need school permission. All you need is imagination and a willingness to grab your rights. There are plenty of other people who want them.

Drug dealers that use beepers have been having some embarrassing moments. A New Jersey dealer had been arrested on cocaine charges when his beeper went off, displaying the number of the person calling. Police called the number and talked to a gentleman who wished to purchase drugs. And guess what those clever cops did!

The beeper is currently sitting on the Camden County Prosecutor's desk. It's still getting calls and the police are still returning them. "We live in a high-tech society," a police officer mused. "Criminals are just as aware of that as we are. These guys are sophisticated. They work very hard at their trade. Illegal as it may be."

We've all heard something about computer viruses by now; most of it undoubtedly inaccurate. Israel, Pakistan, the United States—they're in existence in all kinds of places. And they can screw things up pretty good. We're working on getting an in-depth article on viruses, complete with examples, together for a future issue. In the meantime, there is no reason to panic.

The only people who will have their lives ruined by computer viruses are those that don't take basic safeguards such as backing up and printing out. Once you become completely dependent on a computer, any computer, it's only a

matter of time before a valuable lesson comes your way.

6,900 AT&T customers in New Jersey are being sent 10 extra copies of the AT&T credit cards they ordered. Last month, a runaway computer at AT&T's credit card center in Pleasanton sent out, in separate envelopes, the extra cards.

This is apparently what happened: Some customers complained that they had ordered cards and not received them. To find out if there were more such people, AT&T technicians searched the card division's computer files and came up with a list of about 7,000 names and addresses. The list was "nurt" on an AT&T computer one day in late December to produce electronic orders for the cards. The list should then have been taken out of the computer. Instead, it was left in and continued to run for 10 more days, generating orders for about 10,000 unneeded cards a day.

People who ordered cards got their order, times 11. So people who asked for one got eleven, those who asked for two got 22, etc. Altogether, nearly 100,000 unwanted cards are crawling through the postal service, each in their own envelope.

Our heartiest congratulations to *The Wall Street Journal*, for adopting the 2600 approach to telephones. A recent article about hotel phones noted that most hotels use timers to charge for calls. The timers, according to the paper, don't click on until about 45 seconds after the caller picks up the phone. "If you call home and say 'I'm here,' and hang up immediately, you probably won't be charged," the *Journal* quotes a major hotel senior vice president. "I wouldn't want that to get much publicity, but it's true." The article also notes that hotels remove telephone

(Continued on page 49)

OFFICE OF THE
COMMISSIONER
STATE OF FLORIDA
DEPARTMENT OF REVENUE
TALLAHASSEE, FLORIDA 32399



State of Florida

OFFICE OF THE COMMISSIONER
DEPARTMENT OF REVENUE
TALLAHASSEE, FLORIDA 32399

Florida Revenue Commission

THIS IS A SPECIAL ADVISORY FROM THE FLORIDA PUBLIC SERVICE COMMISSION PLEASE READ CAREFULLY!

Florida has recently implemented the creation of "Payroll Savings" and/or "Pay Rate" long distance telephone contracts. These contracts are available through the company you use for your long distance calls from anywhere in the state. In addition, these contracts often use a payroll savings plan which may be more beneficial to you.

Beware: Many of these companies are operating without authority from the Public Service Commission and you may be not receiving the services you need for, leaving your contract, advance payments, or more. Payroll schemes are often set up to be operated through their retailing approach. As a general rule, the sales agent will encourage you to not only purchase the company's services, but to encourage a sales agent as well. The company will suggest that you can make a lot of money through their multi-level commission plan. While their presentation may appear attractive, it is possible that the company has not been given permission to provide telephone service within Florida if you are approached by a sales agent, or receive literature advertising a "real savings" or a "real pay rate" scheme, be careful.

Florida Law requires that a telephone company must apply for and receive certification from the Florida Public Service Commission before providing long distance service across the state which is not within Florida. In this way, the Florida Public Service Commission is able to regulate and monitor the service the company provides to you, the customer.

Unauthorized companies which are providing telephone service to persons with the state are operating illegally. Your first question regarding a proposed telephone company's services should be "Does your company possess a contract issued by the Florida Public Service Commission?" If the response to this inquiry is "no," we request that you do not proceed any further.

The Commission has been provided in several cases where, if you have any questions or complaints, please contact the Division of Consumer Affairs at 1-800-352-3522 between 7:45 AM and 4:00 PM, Monday through Friday.

Thank You,
George B. Hanna
Division of Consumer Affairs

OFFICE OF THE COMMISSIONER
DEPARTMENT OF REVENUE
TALLAHASSEE, FLORIDA 32399

HAPPENINGS

(Continued from page 38)

charges whenever a guest disputes them. Few guests do this, however.

Bell Canada Enterprises Inc. has gone and changed their name to BCE Inc. as of January 1. They are the parent of Bell Canada, the nation's largest telephone utility. Let's hope it's a change for the better.

U.S. Sprint still can't seem to get its billing system in order. Customers still report not getting bills or getting bills with months' worth of calls on them. Other customers get warning letters saying they haven't paid their bills when it's actually Sprint that hasn't gotten around to processing them. According to some sources, Sprint has been careful not to send warning letters to big customers, regardless of what their records say. So only the small people are falling victim to that blunder.

And finally, in what is perhaps one of the most unfair moves New York Telephone has made in a while, callers who ask a New York Telephone operator for the location of an exchange are now switched to an information operator, for which there is a charge. For the time being, they will warn you that they're doing this. In the near future, they'll just do it, according to a supervisor. It seems a clear and successful attempt at robbing the consumer, who as usual is kept totally in the dark. For those that wish to avoid falling into this trap, we suggest calling an AT&T operator (dial 00) who will provide the information for the proper cost: nothing.

OSUNY

2600 BBS #1

Available 24 hours a day with a wide range of information on computers, telephones, and hacking.

CALL TODAY!

914-725-4060

THE CENTRAL OFFICE

A full range of telephone, radio, computer, and satellite info plus a whole lot more!

2600 BBS #2

914-234-3260

2600 Marketplace

WOULD YOU LIKE TO MAKE SOME MONEY? Big money? Send a business check \$A.5E. to Jeff Duffy, 418 Medford St., Ridley Park, PA 19078. This plan is completely LEGAL.

SOFTWARE FOR IBM COMPATIBLE AND TRAYS COMPATIBLE MODEM. If you are selling or know anyone who is, send replies to Mark St., P.O. Box 7052, Houston, MI 48301-7052.

FOR SALE: Schematics for rod, green, blue and many others. Please write for info to James Surina, 4135 Highland Drive, Megaford, OH 44260.

FOR SALE: Caldera Microline 97 Personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Mark Kelly, 310 Lebold, Lowell, NH 03055.

QUALITY TAP REPRINTS. Complete set (611-97) punched and bound. High quality copies with all special supplements. \$75/set, shipped UPS or USPS or 500/set, shipped Federal Express. Money orders only.

BLCT: BOXING? Let's exchange info on phone numbers, gears, and other things for Blue Box, P.O. Box 117009, Burlingame, CA 94011. Attention: D.C.

payable to Jeff. Do you have something to sell? Are you looking for something to buy? Or

FOR SALE: 8028, multi-T2C, P.O. Box looking for something to buy? Or

1515 Columbia, Trader? This is the place! The 2600

FOR SALE: NE\$6801-515. Marketplace is free to subscribers! cheap, prime

WANTED: C. Send your ad to: 2600 Marketplace, quality \$7.50

FOR SALE: the "Bunker P.O. Box 99, Middle Island, NY 11953. each. Appl.

Home's and include your address label. Only people

FOR SALE: Bluewing font please, no businesses.

by \$492.

FOR SALE: Fabas. If anyone can provide a hard-copy, please send it to JRE, 1647

Greene Dr., Canton, OH 44107.

FOR SALE: TAP BACK ISSUES, complete set Vol. 1-50 of QUALITY copies from originals. Includes schematics and indexes.

still unpaid via UPS or Five Clus

FOR SALE: Mail. Cash/410 sent same day, letters to Rose G., P.O. Box 163, Mt. Laurel, NJ 08054. You are the original, all others are copies!

8028 (CHIP WITH) SPICE STEEL: Files

FOR SALE: diagram are printed - very limited gain. \$15.00 each. Postpaid, check, m.o. to P.E.L. even mail shipped same day, check must clear. Fred G., P.O. Box 663, Mt. Laurel, NJ 08054.

WANTED: Any hacker and pirate

FOR SALE: 8028 (CHIP WITH) SPICE STEEL: Files diagram are printed - very limited gain. \$15.00 each. Postpaid, check, m.o. to P.E.L. even mail shipped same day, check must clear. Fred G., P.O. Box 663, Mt. Laurel, NJ 08054.

WANTED: Any hacker and pirate

FOR SALE: software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to Mark St., P.O. Box 7052, Houston, MI 48301-7052.

FOR SALE: Caldera Microline 97 Personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Mark Kelly, 310 Lebold, Lowell, NH 03055.

BLCT: BOXING? Let's exchange info on phone numbers, gears, and other things for Blue Box, P.O. Box 117009, Burlingame, CA 94011. Attention: D.C.

payable to Jeff. Do you have something to sell? Are you looking for something to buy? Or

FOR SALE: T2C, P.O. Box looking for something to buy? Or

1515 Columbia, Trader? This is the place! The 2600

FOR SALE: NE\$6801-515. Marketplace is free to subscribers! cheap, prime

WANTED: C. Send your ad to: 2600 Marketplace, quality \$7.50

FOR SALE: the "Bunker P.O. Box 99, Middle Island, NY 11953. each. Appl.

Home's and include your address label. Only people

FOR SALE: Bluewing font please, no businesses.

by \$492.

FOR SALE: Fabas. If anyone can provide a hard-copy, please send it to JRE, 1647

The following is a list of routing codes used by AT&T and Bell Operating Companies (BOC) that you can dial for long distance toll-free. The codes are listed by country (USA, Canada, Mexico, Puerto Rico, etc.) where needed. There are codes listed after this list. Codes marked with a * are available to us.

- 000 Rate Quote System (RQS) (1)
- 211-225 Space (13)
- 005-009 Reserved (13)
- 029 RQS
- 010 Reserved
- 211 International Destination Toll Charge (10771) (13)
- 214 Toll-Collecting First (Canada) (2)
- 015-021 Space
- 012-019 Reserved
- 080-085 Space
- 081-081 Reserved
- 089 Space
- 085 Reserved
- 000-099 Space
- 100 Plant Test - Balance Termination
- 112 Plant Test - Test Board
- 113 Plant Test - Signaling Test Operations
- 104 Plant Test - 2-Way Termination and Release Test
- 120 Plant Test - Automatic Termination Handling System/Service Test Line (SSTL)
- 215 Plant Test - RQS Termination Test
- 111 Plant Test - per meter operation
- 106 Plant Test - RQS Echo Support Maintenance
- 105 Plant Test - echo canceled test line
- 110-119 Operator Codes
 - 115 Operator Leave Word
 - 116 Threat OK
- 211 Network Knowledge Center (1)
- 121 Forward Operator (1)
- 122 Area Readline System (4)
- 119 LBO Reserved
- 131 Fireproof Assistance
- 212-217 Reserved
- 113 DSR for Retail Access (1)
- 114-115 Reserved
- 117 Rate and Route (13)
- 142-147 Reserved
- 143 Points not on an HPA - Reporting Service (1)
- 149 Reserved
- 150 State Central (Automatic Assistance) - Hawaii (1)
- 151 International Assistance
- 152-157 Reserved
- 158 Operator Assistance for Equal Access (1)
- 160 International Operator Center (1000) (6)
- 161 Trade Credit Reporting
- 151-157 Reserved
- 161 Points not on an HPA - Canada
- 162-172 Reserved
- 170 Points not on an HPA - Mexico, Hawaii
- 173 Points not on an HPA - Canadian Territory, Puerto Rico, Virgin

Canada (Canada 202)

- 131 Reserved
- 114 Cable Control (Automatic Assistance) - Ottawa
- 115 Reserved
- 116 Points not on an HPA - Canada, Mexico
- 117-118 Reserved
- 119 Points not on an HPA - Canada
- 120 Points not on an HPA - Mexico, Canada
- 121 Toll Station
- 122 International Switching Center (155) - Voice Mailbox (1)
- 123 LBO - New York, 2024
- 124 LBO - Pittsburgh
- 125 LBO - Atlanta, 017
- 126 LBO - Sacramento
- 127 LBO - Sacramento (Voice) (13)
- 128 LBO - New York, 2020
- 129 Points not on an HPA - Mexico City, Mexico
- 130 Points not on an HPA - Mexico, Mexico
- 131 Conference Loop Around
- 131 Area Reserved 800 (Language) - Reporting Service (1)
- 132 Reserved
- 133 LBO - Central (Reporting Assistance) - Ottawa
- 134 LBO - New York, 2020, Mexico
- 135 Area Reserved 800 (1)
- 136 Area International 800 (4)
- 141 Reserved
- 142 Area International City Service Center (155)
- 143 Cable Control (Automatic Assistance) - Alaska
- 144 Area 202 (202) (1)

4 or 5 digit codes (1)

- 119-2222 Universal or Toll Callers
- 211-1111 Conference Operator (1)
- 1225-1231 Mobile Telephone Service
- 210-1151 Service Bell/Service (1)
- 224-1151 Toll Terminal
- 015-1155 Day and Night Assistance
- 015-1156 Mail/Parcel Follows
- 115-1157 2-Way Service Test
- 115-1158 Service - Computer Assistance (1)
- 115-1159 Service - Long Term Reservation (1)
- 115-1160 Calling Card Assistance and Rate Equipment (1)
- 115-1161 Calling Card Assistance - Free Assistance
- 115-1162 Calling Card Assistance - Toll-Free Agency (1)
- 115-1163 Calling Card Assistance - Toll-Free Agency (1)

00223:

(1) The Rate Quote System is a voice response system used by operators to obtain correct information. The system, which is used only when needed as an alternative to calling the toll-free operator, requires a toll-free number, routing information and a geographical area code response. See the page in this publication for details on toll-free routing information and codes.

Continued on next page

